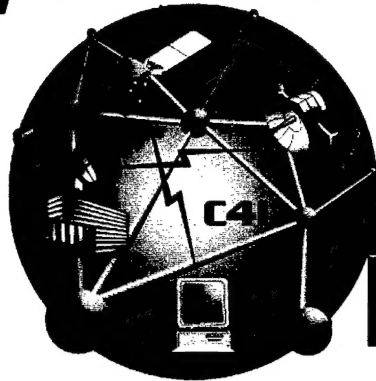


# ***Joint Warrior Interoperability Demonstration 1997 Assessment Report***

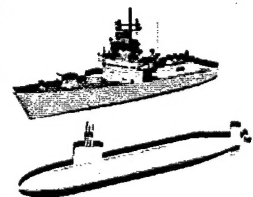


**VALUE ADDED**



**MISSION  
SUCCESS**

**DISTRIBUTION STATEMENT E**  
Approved for public release  
Distribution Unlimited



**Defense Information Systems Agency  
D8 C4I Modeling, Simulation, and Assessment  
Arlington, Virginia**

**19971212 022**

**DEFENSE INFORMATION SYSTEMS AGENCY  
D8 C4I MODELING , SIMULATION, & ASSESSMENT**

**JOINT WARRIOR INTEROPERABILITY DEMONSTRATION 97  
(JWID 97)**

**FINAL REPORT**

**October 10, 1997**

**Submitted by:**

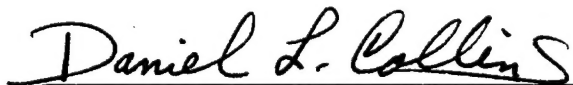


**ROGER K. PRATT**

**MAJ, USA**

**Chairman, Assessment Working  
Group**

**Approved by:**

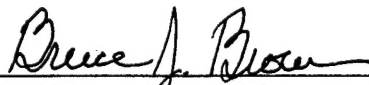


**DANIEL L. COLLINS**

**Lt Col, USAF**

**Chief, CINC Support Division (D82)**

**Approved by:**



**BRUCE J. BROWN**

**Deputy Director**

**C4I Modeling, Simulation and  
Assessment (D8)**

## PLEASE CHECK THE APPROPRIATE BLOCK BELOW:

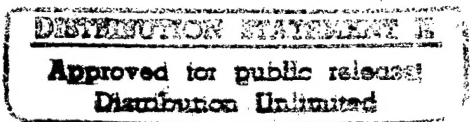
- AO #  
☒ ONE copies are being forwarded. Indicate whether Statement A, B, C, D, E, F, or X applies.
- ☒ DISTRIBUTION STATEMENT A:  
 APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED
- ☐ DISTRIBUTION STATEMENT B:  
 DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES ONLY; (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).
- ☐ DISTRIBUTION STATEMENT C:  
 DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS; (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).
- ☐ DISTRIBUTION STATEMENT D:  
 DISTRIBUTION AUTHORIZED TO DoD AND U.S. DoD CONTRACTORS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).
- ☐ DISTRIBUTION STATEMENT E:  
 DISTRIBUTION AUTHORIZED TO DoD COMPONENTS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).
- ☐ DISTRIBUTION STATEMENT F:  
 FURTHER DISSEMINATION ONLY AS DIRECTED BY (Indicate Controlling DoD Office and Date) or HIGHER DoD AUTHORITY.
- ☐ DISTRIBUTION STATEMENT X:  
 DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND PRIVATE INDIVIDUALS OR ENTERPRISES ELIGIBLE TO OBTAIN EXPORT-CONTROLLED TECHNICAL DATA IN ACCORDANCE WITH DoD DIRECTIVE 5230.25, WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA FROM PUBLIC DISCLOSURE, 6 Nov 1984 (Indicate date of determination). CONTROLLING DoD OFFICE IS (Indicate Controlling DoD Office).
- ☐ This document was previously forwarded to DTIC on \_\_\_\_\_ (date) and the AD number is \_\_\_\_\_.
- ☐ In accordance with provisions of DoD instructions, the document requested is not supplied because:
- ☐ It will be published at a later date. (Enter approximate date, if known).
- ☐ Other. (Give Reason)

DoD Directive 5230.24, "Distribution Statements on Technical Documents," 18 Mar 87, contains seven distribution statements, as described briefly above. Technical Documents must be assigned distribution statements.

Lt Col Daniel L. Collins, USAF, Ph.D.  
 Print or Type Name

Lt Col Daniel L. Collins, USAF, Ph.D.  
 Authorized Signature/Date

703-696-9292  
 Telephone Number

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 10 OCT 1997	3. REPORT TYPE AND DATES COVERED 14 July - 10 Oct 1997		
4. TITLE AND SUBTITLE Joint Warrior Interoperability Demonstration 1997 Assessment Report		5. FUNDING NUMBERS Project 011		
6. AUTHOR(S) Pratt, Roger K., Major, USA, Collins, Daniel L. Lt Col, USAF, Ph.D., Brown, Bruce J.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Information Systems Agency (D82) CINC Support Division 3701 N. Fairfax Drive Arlington VA 22203		8. PERFORMING ORGANIZATION REPORT NUMBER DISA D82-01		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Information Systems Agency D8 C4I Modeling, Simulation and Assessment Directorate 3701 N. Fairfax Drive Arlington VA 22203		10. SPONSORING/MONITORING AGENCY REPORT NUMBER		
11. SUPPLEMENTARY NOTES The CINC Support Division of DISA was tasked to develop methodology for assessing new C4I Technology, collecting and analyzing the data, and writing up the results for 28 technology demonstrations.				
12a. DISTRIBUTION/AVAILABILITY STATEMENT No Restrictions		12b. DISTRIBUTION CODE		
				
13. ABSTRACT (Maximum 200 words) The Joint Warrior Interoperability Demonstration for 1997 (JWID 97) provided a unique environment for the Warfighter to identify the value added for mission accomplishment of demonstrated C4I capabilities. A Warfighter focused assessment was achieved through the use of: 319 highly qualified Coalition military operators and staff; demonstrations that were exercised with scenario driven play for repeatability of processing and product development; and a skilled analysis team augmented with automated data collection and analysis tools. This assessment process enabled a comprehensive assessment of new technologies, enhanced systems and new systems in an operational, bandwidth constrained, multi-national environment and an initial look at C4I capabilities needed to support network-centric warfare. Twenty-eight demonstrations participated in JWID 97 to provide solutions for ten objectives. These objectives reflected technical issues that currently exist in the USACOM Area of Responsibility (AOR) and provided JWID 97 with the opportunity to demonstrate solutions to real-world problems.  We would like to thank the Site Directors for providing the operator and staff personnel who made this assessment possible and our Coalition partners for their input into the assessment. Finally to Admiral Fallon, who made a personal effort, visiting the sites, to ensure experienced warfighters were available and understood their primary mission was to assess the demonstrations.				
14. SUBJECT TERMS Telecommunications and Information Management, COTS, GOTS, DII Common Operational Environment, JWID97 Assessment Report		15. NUMBER OF PAGES 95		
		16. PRICE CODE		
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	



## **REPRODUCTION QUALITY NOTICE**

**This document is the best quality available. The copy furnished to DTIC contained pages that may have the following quality problems:**

- **Pages smaller or larger than normal.**
- **Pages with background color or light colored printing.**
- **Pages with small type or poor printing; and or**
- **Pages with continuous tone material or color photographs.**

**Due to various output media available these conditions may or may not cause poor legibility in the microfiche or hardcopy output you receive.**

☒ **If this block is checked, the copy furnished to DTIC contained pages with color printing, that when reproduced in Black and White, may change detail of the original copy.**

***EXECUTIVE SUMMARY***  
***JOINT WARRIOR INTEROPERABILITY DEMONSTRATION FOR 1997***  
***ASSESSMENT REPORT***

---

The Joint Warrior Interoperability Demonstration for 1997 (JWID 97) provided a unique environment for the Warfighter to identify the value added for mission accomplishment of demonstrated C4I capabilities. A Warfighter focused assessment was achieved through the use of: 319 highly qualified Coalition military operators and staff; demonstrations that were exercised with scenario driven play for repeatability of processing and product development; and a skilled analysis team augmented with automated data collection and analysis tools. This assessment process enabled a comprehensive assessment of new technologies, enhanced systems and new systems in an operational, bandwidth constrained, multi-national environment and an initial look at C4I capabilities needed to support network-centric warfare. Twenty-eight demonstrations participated in JWID 97 to provide solutions for ten objectives. These objectives reflected technical issues that currently exist in the USACOM Area of Responsibility (AOR) and provided JWID 97 with the opportunity to demonstrate solutions to real-world problems.

The top ten rated demonstrations are recommended for accelerated development and procurement as a result of the warfighter assessment. They are grouped into three categories: gold nuggets, enhancements to existing systems, and new technologies. Four of the top ten demonstrations were identified as gold nuggets - capabilities that were ready for immediate Warfighter use that could be available within 6 months after funding. These included: a) Increased Compression Engine (ICE): capability to compress and transfer images quickly, with little loss of image integrity; b) COMPASS: capability to access distributed legacy modeling and simulation tools and use distributed collaborative planning tools to support Warfighter plan development, preview, revision, and rehearsal; c) Submarine Combat Operations: capability to significantly increase submarine accessibility to commanders through increased bandwidth; and d) Radiant Mercury Imagery Guard (RMIG): capability to automatically screen and guard the transfer of National Imagery Transmission Format (NITF) Standard images between various security levels.

Three of the top ten demonstrations provided significant enhancements to established programs. These included: enhancements to JDISS to support multi-level security operations; enhancements to the common operational picture to make it more complete; and enhancements to the Global Broadcasting System (GBS) reachback services in support of tactical users.

The remainder of the top ten demonstrations provided new technologies that provided value added to the warfighter but require further refinement and assessment. These included capabilities to provide real-time location information derived from GPS disseminated via UHF LOS and UHF SATCOM (SABER); capabilities to access, deliver, and retrieve imagery and geospatial information (NIMA); and capabilities to integrate real-time network monitoring and intrusion detection with automated assessment tools.

Several infrastructure and compatibility issues were also addressed during JWID. The Coalition Wide Area Network (CWAN) handled Coalition releasable information. The CWAN demonstrated connectivity between US and Allied sites as peers and fully supported collaboration between all participants. Any necessary security separation occurred between the CWAN and country assets. Warfighter assessment confirmed that this topology is the only efficient way to support network centric warfare. Multi-Level Security (MLS) solutions were demonstrated during JWID and some accredited solutions exist. The benefits of information accessibility and distributed collaborative planning, unencumbered by security delays, are within reach. A concerted effort needs to be made to bridge the gap in data labeling and MLS issues. Email was used to pass JWID traffic and the concept proved to be valuable, although the lack of procedures, policy and discipline caused some initial problems. Collaborative planning tools were not compatible among demonstrations. The continued proliferation of distributed collaborative planning tools that are not interoperable thwarts the concept of distributed collaborative planning and requires some standardization issues to be resolved in the future.

JWID 97 provided an environment for the Warfighter operator and staff, sponsor, and industry to work together to identify value added C4I technologies and to experiment with new technologies and procedures for network-centric warfare. New technologies and concepts were explored and scenario play allowed the warfighter to attempt creative methods to use the demonstrations to solve current problems.

(This page intentionally left blank)

## ***ACKNOWLEDGMENT***

---

The Assessment Working Group would like to thank the JWID Joint Program Office and CINCUSACOM for their efforts to ensure that the assessment of JWID 97 was a success. Their support and focus on the assessment as the end result of the JWID process and providing for a consolidated assessment have made this assessment a success.

We would also like to thank all the members of the assessment team for their input to the process and their help in collecting and analyzing the warfighter assessment data: USACOM J6, the Joint Battle Center, and the Naval Post Graduate school. This mammoth effort would not have been possible without their support.

We would like to thank the Site Directors for providing the operator and staff personnel who made this assessment possible and our Coalition partners for their input into the assessment. Finally to Admiral Fallon, who made a personal effort, visiting the sites, to ensure experienced warfighters were available and understood their primary mission was to assess the demonstrations.

(This page intentionally left blank)

## TABLE OF CONTENTS

Executive Summary .....	ii
Section 1 - Introduction .....	1-1
1.1 Background.....	1-1
1.2 Purpose .....	1-1
1.3 Objectives .....	1-2
1.4 Scenario .....	1-2
1.5 Warfighter Assessment Process.....	1-3
1.6 Document Structure .....	1-5
Section 2 - Assessment Results .....	2-1
2.1 Objective Results.....	2-3
Objective One - Multi-Level Security .....	2-4
Objective Two - Telecommunications and Information Management .....	2-6
Objective Three - Dominant Battlespace Awareness .....	2-8
Objective Four - Sensor to Shooter.....	2-10
Objective Five - Information Warfare and Operations .....	2-12
Objective Six - COTS/GOTS Technology.....	2-13
Objective Seven - DII Common Operational Environment .....	2-14
Objective Eight - Integrated Logistics Support .....	2-15
Objective Nine - Integrated Single Computer Operations .....	2-16
Objective Ten - Year 2000.....	2-17
2.2 Special Interest Areas.....	2-19
Coalition Wide Area Network.....	2-20
Electronic Mail.....	2-22
Global Command and Control System (GCCS) .....	2-24
2.3 Demonstration Assessments .....	2-27
JW002 MECCS.....	2-28
JW004 Paralon PathKey .....	2-30
JW008 3D Volumetric Display .....	2-32
JW009 ICE.....	2-34
JW011 Cellular Communications.....	2-36
JW012 JCSE.....	2-38
JW015 JDISS.....	2-40
JW023 COMPASS .....	2-42
JW028 JSTARS .....	2-44
JW032 SABER.....	2-46
JW036 Sensor Box .....	2-48
JW039 Battlefield VTC .....	2-50
JW043 JACCS .....	2-52
JW044 3D Battlespace Visualization .....	2-54
JW045 Imagery and Geospatial Support .....	2-56
JW052 Information Operations Defense .....	2-58
JW060 Trusted Coalition Database .....	2-60
JW068 Deployable JFACC .....	2-62
JW073 Joint C4ISR.....	2-64
JW074 JMCOMS .....	2-66
JW080 Submarine Joint Coalition Operations .....	2-68
JW085 Integrated Situation Awareness .....	2-70
JW086 Joint Sensor to Shooter .....	2-72
JW089 Theater Deployable Communications .....	2-74
JW101 Defense Message System.....	2-76
JW106 Global Combat Support System (GCSS) .....	2-78
JW112 Enhanced Broadcast Services.....	2-80
JW123 Radiant Mercury Image Guard.....	2-82
Section 3 - Conclusions and Recommendations .....	3-1

3.1 Candidates for Implementation.....	3-1
3.1.1 Gold Nuggets .....	3-1
3.1.2 Enhancements to Existing Systems .....	3-2
3.1.3 New Technologies.....	3-4
3.2 Issues .....	3-5
3.3 Recommendations .....	3-5
Appendix A - Acronym List.....	A-1



---

---

## ***SECTION 1 - INTRODUCTION***

---

---

(This page intentionally left blank)

## SECTION 1 - INTRODUCTION

---

This document provides an assessment of the Joint Warrior Interoperability Demonstration for 1997 (JWID 97). There were a total of 28 demonstrations that were selected to help provide solutions for 10 identified objectives. These objectives reflected the joint technical issues that exist in the in the United States Atlantic Command (USACOM) Area of Responsibility (AOR) and provide JWID 97 with the opportunity to demonstrate solutions to real world problems.

### 1.1 Background

---

Since the late 1980's, a series of annual demonstrations have focused on providing the Joint warfighting community with innovative advances in Command, Control, Communications, Computers, and Intelligence (C4I) systems. JWID 97 was the ninth in the series, and is built on those efforts to display advances in technology, networking, and interoperability through the environment of a Coalition Joint Task Force (CJTF) deployment.

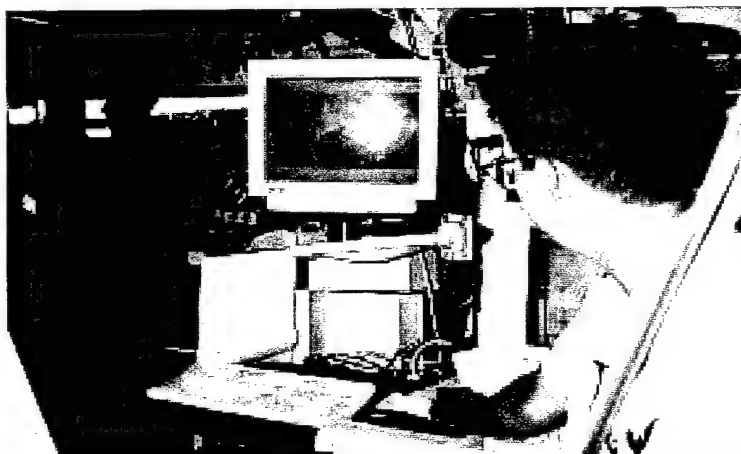


JWID 97 was a cooperative, multi-service, and Allied demonstration that was designed to show interoperability among forces and C4I systems with emphasis on Command and Control (C2) architectures. The Joint Staff J6 was the overall sponsor and the U.S. Navy was the lead service for this demonstration. USACOM acted as the host Commander-in-Chief (CINC) with the services, Agencies and Allies participating at various sites in the United States, both on land and at sea. The Allied participants included Australia, Canada, North Atlantic Treaty Organization (NATO), New Zealand, and the United Kingdom.

### 1.2 Purpose

---

In times of increasingly scarce resources, JWID provides a Joint and multinational environment for both developer and the warfighters to cooperatively solve technical and procedural issues associated with the fielding of new C4I capabilities. The developer interfaces with actual system operators, and command and staff personnel that use the demonstrated system's products. Operators, commanders, and staff are exposed to future technologies that may solve problems that exist in the accomplishment of their mission tasks. Developers, operators, and staff are placed in a scenario based environment that facilitates potential solutions for problems previously identified by the CINC and lead service. The scenario allows an assessment of systems: a) in an environment that approaches real operations; b) provides a basis for sound feedback to developers; c) allows warfighters to evaluate solutions that are ready for fielding. The JWID assessment process results in the identification of solutions for objectives that can be fielded in the short term, as well as those that need additional development.



### **1.3 Objectives**

---

JWID 97 operations were based on ten objectives. The objectives were used to select demonstrations that had potential in solving known problems in the CINC AOR and resulted in a selection of 28 demonstrations for JWID 97. These objectives are listed below.

1. Demonstrate real-time and seamless information exchange between multiple levels of security at the Commander Coalition Task Force (CCTF) and component level, particularly for the purpose of C2 and collaborative planning.
2. Demonstrate innovative telecommunications and information management technology that enhances data delivery to and from Joint Warriors at the unit level, particularly Common Operational Picture (COP) and imagery.
3. Demonstrate tailorable Dominant Battlespace awareness (including 3-D) in a Coalition Task Force (CTF) setting, highlighting multimodal data fusion, COP track correlation and management.
4. Demonstrate sensor-to-sensor and sensor-to-shooter technologies to enhance combat identification and theater missile defense in a Coalition environment, and to provide targeting information for stand-off and precision guided munitions utilizing selected portions of the Joint Requirements Oversight Council (JROC) approved precision strike C4I architecture.
5. Demonstrate technologies that enhance information superiority through the use of Information Operations/Information Warfare (IO/IW). These technologies should provide assurance of Coalition access, use, and integrity of C4I Surveillance and Reconnaissance (C4ISR) systems while preventing unauthorized use of the same.
6. Demonstrate the ability of Commercial-Off-The-Shelf (COTS)/ Government-Off-The-Shelf (GOTS) technology to provide constant data exchange with in-garrison, in-transit, and deployed elements of the CTF.
7. Demonstrate enhancements to the Defense Information Infrastructure (DII) that improves its utility and interoperability to the CTF.
8. Demonstrate an integrated, near real-time focused logistics system with a planning and decision support capability. The system should track all classes of supply, prepositioned war reserve assets, and personnel to/from the sustaining base and wholesale depots.
9. Demonstrate the ability to provide an integrated solution for all tactical and non-tactical applications of a single PC.
10. Demonstrate the ability of Information Technology to identify and solve millennial problems in order to operate beyond the year 2000.

### **1.4 Scenario**

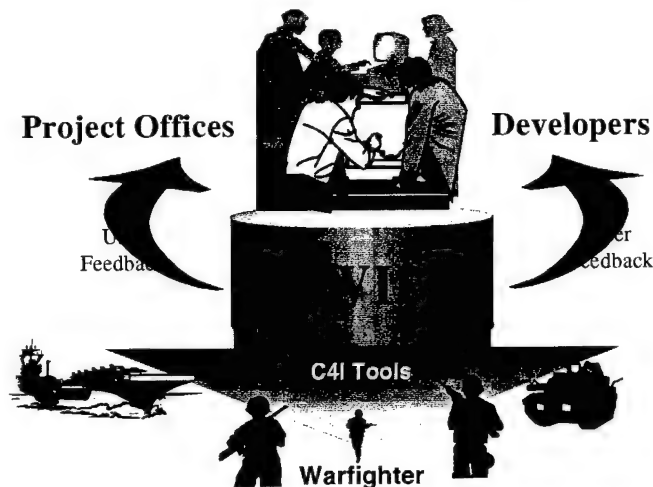
---

The JWID 97 scenario provided the context and situational framework that defined the operational boundaries for data interchange and interoperability to support the demonstration functional assessment. The scenario, which employs seven of the eight phases used in the USACOM 1996 "Purple Star" Exercise, provided the warfighters backdrop for evaluating demonstrations within an adapted Operational Concept for Coalition Warfare. The scenario demonstrated to warfighting commanders and acquisition decision-makers relevant new interoperability technology and the utility of evolving systems for operation use in a Coalition environment.

JWID 97 was a US and Allied Coalition operation led by the Commander, Carrier Group Six who acted as the CCTF conducting Combined Operations at the Joint Component Commander Level. CINCUSACOM was the host CINC operating from the Joint Battle Center (JBC) at the Joint Training Analysis and Simulation Center (JTASC) in Suffolk, Virginia. The CCTF and his staff operated from the USS John C. Stennis (CVN 74).

During all phases, Coalition forces faced a notional IW and terrorism threat. The notional force structure consisted of combined Joint and Allied ground, air, and maritime components which included a carrier battle group with two nuclear powered attack submarines and an amphibious task force. These forces conducted combined operations which included a show of force, amphibious assaults, and Theater Ballistic Missile Defense (TBMD) offensive and defensive operations. The CCTF remained aboard the USS John C. Stennis throughout the scenario operations.

## 1.5 Warfighter Assessment Process



### Purpose

- Speed C4I technologies to the Warfighter.
- Provide warfighter feedback to developers/ project offices on ways to improve and enhance systems and applications to be more responsive to customer needs.
- Identify new technologies that demonstrate potential in meeting warfighter requirements.

### 1.5.1 Assessment Tasking and Team Membership

Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6260.01 tasks the Defense Information System Agency (DISA) to conduct a functional and technical assessment of all JWID demonstrations. In JWID 97, DISA was joined by ACOM J6 and the JBC in a partnership to conduct the JWID assessment. The assessment execution was accomplished through a team effort of over 60 people with representatives from DISA, Joint Interoperability Test Command (JITC), ACOM, JBC, the Joint Staff, the JWID Project Office and students from the Naval Postgraduate School, contributing to the collection and analysis of qualitative and quantitative data.

### 1.5.2 Assessment Methodology

The methodology was designed to produce an assessment using warfighter insight into systems that have no formal requirements. Three major goals were developed to ensure that the assessment would provide useful and meaningful results. These goals were to ensure that: a) insure that the operators and staff that made the assessments had the right experience to provide meaningful input. b) the right data was collected. c) data collection and analysis tools were available to support collection and analysis. Figure 1-1 provides an overview of the assessment process.

For JWID 97, CINC headquarters, CCTF and all components were staffed by more than 319 US and Allied soldiers, sailors, airmen and marines, experienced in the required functional areas. Enlisted personnel had an average of 9 years experience; officers has an average of 13 years experience. Training was provided on the use of the systems prior to the start of JWID. During the final three weeks of JWID, operators interacting with the staff, performed functions in their specialty

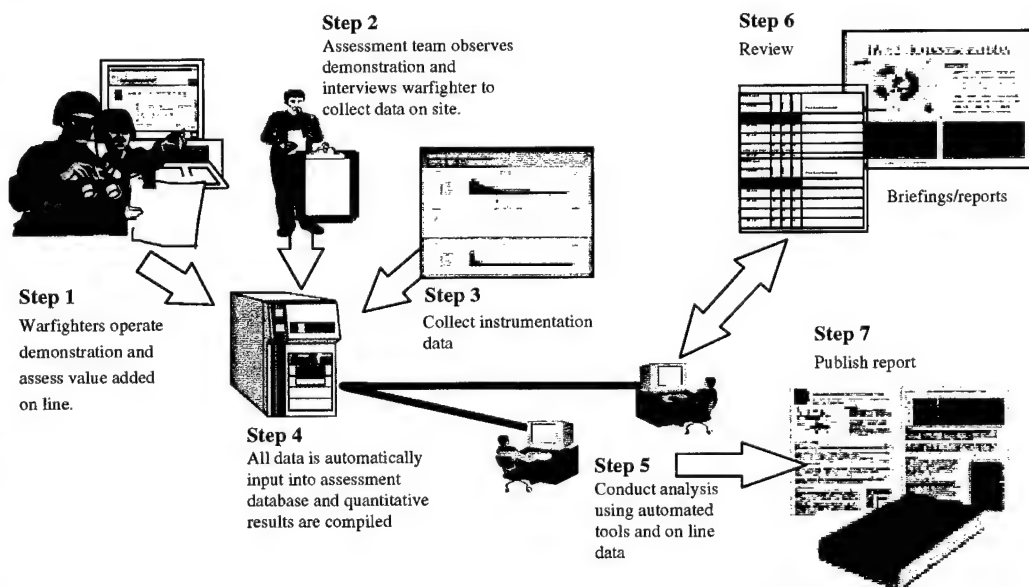


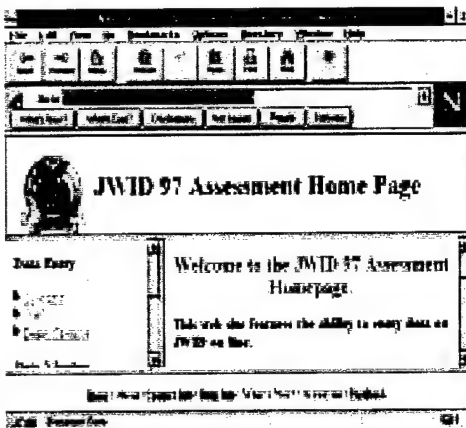
Figure 1-1. Assessment Process

areas to provide the flow of information to the commander. The scenario was used to drive requirements to force decisions from the commanders and supported interaction between the JWID demonstrations. Admiral Bucchi, the senior warfighter solicited warfighter utility from the component commanders, which corroborated the assessment results that the operators and staff had input into the database and comment sheets.

Table 1-1 Measures of Effectiveness

<b>Usefulness MOEs: <i>Does this demonstration provide a required capability to support the warfighter?</i></b>
<ul style="list-style-type: none"> <li>• Value Added: The ability to increase the fulfillment of a mission or function as compared to performing them by the current method.</li> </ul>
<ul style="list-style-type: none"> <li>• Completeness: The ability to provide all necessary information on an area of interest needed to accomplish the missions or functions.</li> </ul>
<ul style="list-style-type: none"> <li>• Interaction: The ability to permit workstations and nodes to responsively collaborate in monitoring, assessing, and executing mission and functions.</li> </ul>
<ul style="list-style-type: none"> <li>• Accuracy: The ability to provide information that is free from error.</li> </ul>
<ul style="list-style-type: none"> <li>• Human Factors: The ability of the system software and hardware to provide the operator with a machine interface which is easy to relate to and use.</li> </ul>
<ul style="list-style-type: none"> <li>• Consistency: The ability to present common information and indicators.</li> </ul>
<ul style="list-style-type: none"> <li>• Interoperability: The ability of the system to facilitate the direct electronic exchange of information and services with other systems.</li> </ul>
<ul style="list-style-type: none"> <li>• Accessibility: The ability to locate and retrieve information in databases, get to local or remote applications, services, and work files.</li> </ul>
<ul style="list-style-type: none"> <li>• Standards Compliance: The ability of a system to comply with the DII COE, the GCCS/GCSS COE, or other commercial standards (Win95, NT, Internet, etc.)</li> </ul>
<ul style="list-style-type: none"> <li>• Year 2000 Operational Capability: The ability of a system to fully operate without interruption beyond the year 2000.</li> </ul>
<ul style="list-style-type: none"> <li>• Availability: The ability of a system to be continuously operational to accomplish mission and functions.</li> </ul>
<ul style="list-style-type: none"> <li>• Bandwidth: The ability to work using limited communications resources to perform required missions and functions.</li> </ul>

Based on the use of the systems in this operational environment, after each of the three scenario runs, operators and staff personnel completed questionnaires that captured data on the utility and ease of use of the system. Qualitative comments to support the questionnaire data were also collected. Information was collected and categorized in three areas: usefulness, usability, and performance. These areas are depicted in table 1-1 above. Usefulness was used to determine the utility of a capability and its products and services to enhance the warfighters ability to accomplish the required functions and missions. The measures of effectiveness used to collect usefulness data included value added, completeness, interaction, and accuracy. Usability measures included human factors, consistency, interoperability, and accessibility. Performance measured the availability of the system and its compliance with DII Common Operational Environment (COE) criteria, as well as the collection of bandwidth data. Questionnaires were specifically designed to capture the usefulness, usability and performance assessment by the warfighters of the systems/applications. These questionnaires have been developed through warfighter pretesting. They have been statistically tested to ensure the accurate measurement of warfighter assessment. Although it has been determined through statistical analysis that usefulness and usability both measure the same dimension, they have been reported individually in this document to be consistent with past JWID results. Demonstration specific capabilities that were to be assessed were also with the developers of the systems to ensure that the systems in JWID could perform all the functions that were listed in their demonstration plans. These capabilities were categorized either as critical or non-critical. Critical tasks were defined as essential functions needed to show value added to the Warfighter.

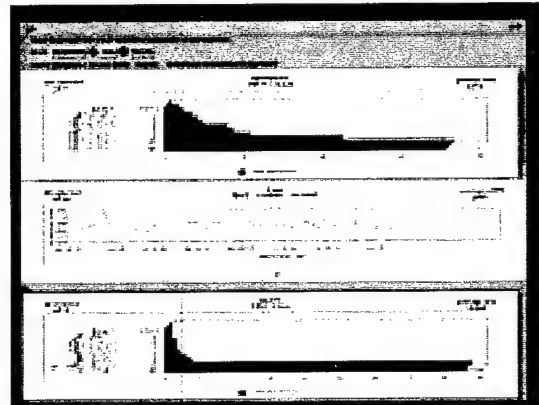


## Automated Assessment Tools

On-line web-based data entry allowed the warfighter to complete questionnaires and provide comments from their workstations as the demonstration was running. Automatic storage to the developed assessment database allowed initial analysis of the assessment data in real time. Probe-based technology was used to automatically collect bandwidth used by each of the demonstrations.

The assessment process employed technology to assess the demonstrations and make the job of analyzing the thousands of inputs easier and more timely. An easy to use, on-line web site was used to allow the warfighter to access and fill out questionnaires and observation forms from their demonstration workstations. This information was collected automatically in a newly developed database that fed analysis reports to on-site analysts for review. Over 6000 pages of text and 2000 questionnaires were input into the database.

After collection, the assessment team members reviewed on a daily basis the warfighter assessment data and comments through the use of preformatted queries and reports so that additional information or clarification of issues could be collected. The analysts also performed system capability checks in which the operators demonstrated all capabilities that were being assessed. New technology was introduced that allowed bandwidth data to be automatically collected through the use of on-line probe based instrumentation. Several sites were successfully instrumented, despite acquisition delays, to collect data during the assessment phase. This data produced valuable information on usage of the Local Area Network (LAN) and network resources.



### 1.5.3 Reporting Process

Initial scores and results for each of the demonstrations were compiled and reported to the Senior Management Group within hours of the completion of JWID. This initial look was finalized over the next four weeks into the assessment briefing and report. These final results were briefed to the JWID participants and the Senior Management Group the week on 11 September 1997. At this time, the golden nugget list was developed based on the assessment results. These results and the golden nuggets were then briefed to the CINCUSACOM. These results will be briefed to the Joint Chiefs of Staff (JCS).

## 1.6 Document Structure

The JWID 97 Assessment Report consists of three sections. Following this introductory section, Section 2 addresses the assessment results by objective. It includes assessment results of each objective and an assessment of the special interest areas, including email, the Coalition Wide Area Network (CWAN) and Global Command and Control System (GCCS). Section 3 contains the high level conclusions and recommendations for all demonstrations and identifies those demonstrations that were assessed to have the highest potential to provide value added to the warfighter.

Appendix A contains a list of acronyms used in this document.

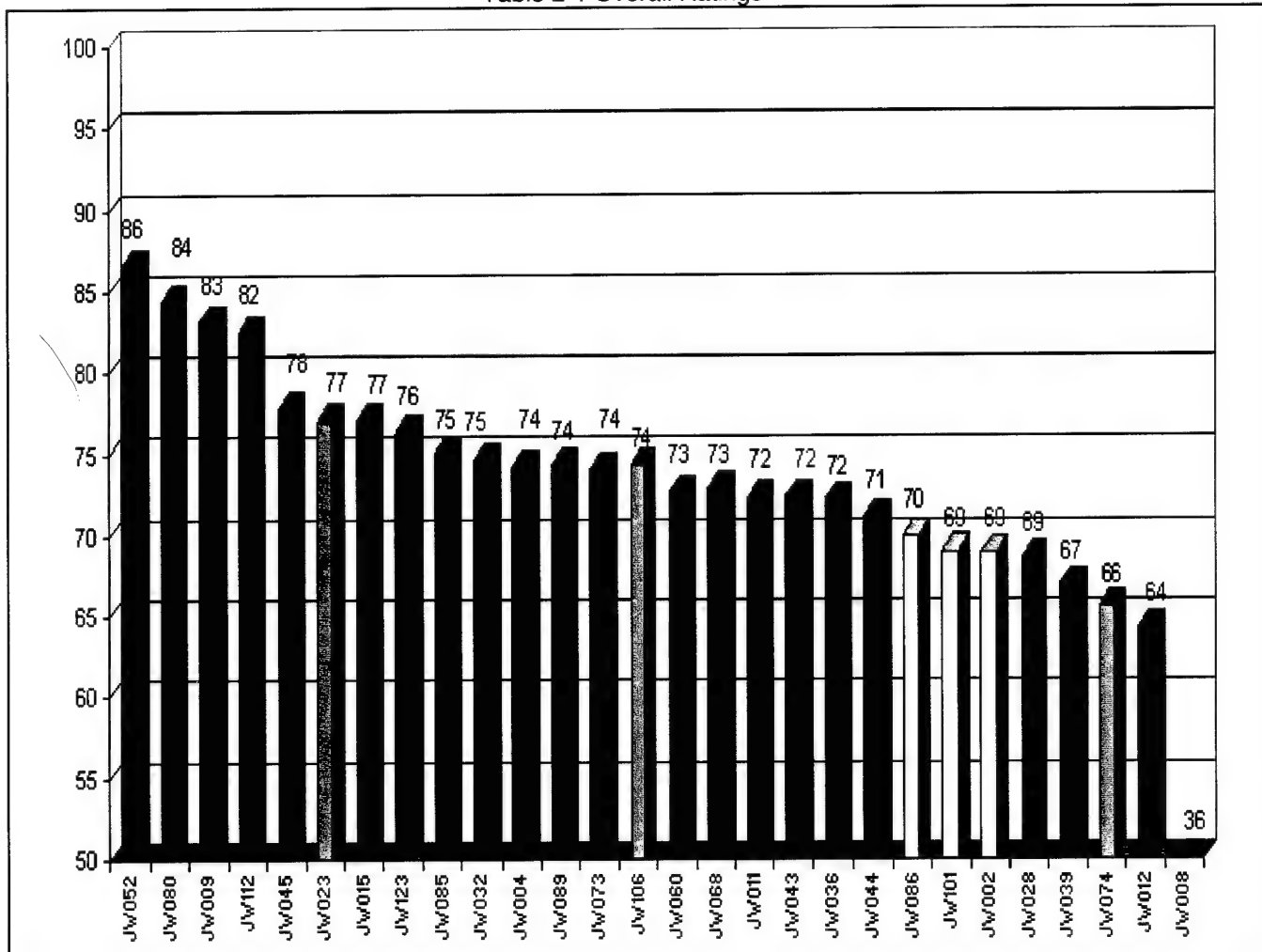


(This page intentionally left blank)

## SECTION 2 - ASSESSMENT RESULTS

This section of the report addresses results by objective, special interest area, and by individual demonstration. Each of these areas is addressed in a short summary, which describes the objective, special interest area, or demonstration and discusses the major results, conclusions and recommendations. A summary of the results for each demonstration is depicted below Table 2-1. The percentages represent the average of the warfighter assessment of usefulness, usability and performance. Demonstration reports in this section have the individual scores for each demonstration.

Table 2-1 Overall Ratings



(This page intentionally left blank)

---

---

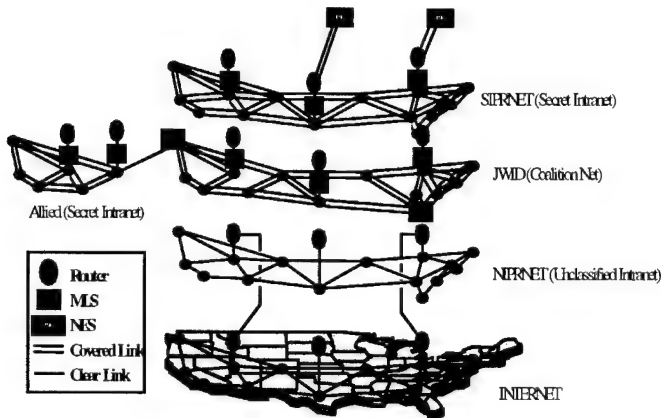
## ***2.1 OBJECTIVE RESULTS***

---

---

# Objective 1

## Multi-Level Security



### Objective Statement

- Demonstrate real-time information exchange between multiple levels of security (MLS) at the Coalition Task Force (CTF) and component level, particularly for the purposes of C2 and collaborative planning.

### Technical Challenges

- Demonstrate automated sanitization of information and security purposes.
- Demonstrate Allied/Coalition interoperability and collaboration among all Joint Task Force (JTF) components using all classification levels.
- Demonstrate how U.S. only information within the GCCS COE can be automatically sanitized and released to our Allied/Coalition partners.
- Demonstrate a C4I system that is DII COE compliant, focused on real-time data exchange; incorporate Web browser technology to facilitate interoperability between U.S. and Allied/Coalition forces.
- Demonstrate Multi-Level Security (MLS).
- Make all Allied Forces command and control systems releasable to Coalition forces.
- Demonstrate modeling and simulation tools in support of Theater Ballistic Missile Defense, Collaborative Action Planning, and other battlefield functional areas.

### Results

Demo #	Supported Objective	Remarks
JW004		Not linked to the CWAN.
JW015	•	Real-time exchange between multiple levels of security.
JW036		Did not exchange information between multiple levels of security.
JW043	•	Real-time exchange between the CTF and the Component Level.
JW045	•	C2 Guard provided sanitation mechanism for imagery made available to GCCS/COE.
JW060	•	Trusted Database provided real-time view of the battlespace across security levels; MLS capability.
JW068		Did not exchange information between multiple levels of security.
JW073	•	Real-time exchange between multiple levels of security.
JW074		Did not exchange information between multiple levels of security.
JW080		Did not exchange information between multiple levels of security.
JW085		Did not exchange information between multiple levels of security.
JW086	•	Met the technical challenge of modeling and simulation.
JW123	•	Screened imagery headers and automatically guarded the real-time exchange between multiple levels of security.

- = Indicates that one or more of the technical challenges were met

**JW015** - Provided an integrated family of plug-in intelligence support and multimedia collaborative software segments based on DII COE, and COTS MLS and Trusted Web technology on a single workstation. JDISS allowed the secure exchange of intelligence data and multi-security level access to web-based products and data. All applications were provided on both NT and UNIX platforms, except the Multi Network Workstation (MNV) was not available on the NT JDISS terminal. It also provided non-tactical applications on these workstations as well.

**JW043** - Demonstrated real-time information exchange at the Coalition Task Force (CTF) and component level by providing real-time data exchange incorporating web browser technology to facilitate interoperability between US and Allied/Coalition forces. Use of the Joint Attack C2 System (JACCS) COTS web server, within an operational facility (OPFAC), promoted vertical and horizontal interoperability within the coalition and joint framework via selected views of OPFAC databases through the use of commercial web browsers. This provided real-time availability of time sensitive maneuver and fire support information to Joint and Coalition elements.

**JW045** - Transferred imagery and geospatial data to the CWAN from the Secret Internet Protocol (IP) Network (SIPRNET) via the Information Dissemination Management (IDM) server and C2 Guard. The CWAN server, via the C2 guard, received no improperly marked images.

**JW060** - Provided a concept to provide real-time and seamless information exchange between multiple levels of security at the CTF and component level through use of the Trusted Coalition Scenario Database (TCSdb).

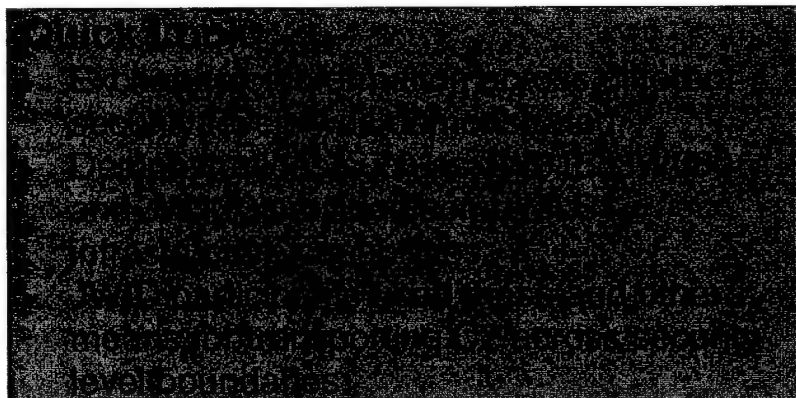
**JW073** - Demonstrated the exchange of near real-time (non-) releasable Intelligence, Surveillance, and Reconnaissance (ISR), force asset and mine/minefield data between US and combined Joint Counter Mine (JCM) forces. Data security levels ranged from non-releasable Top Secret (TS)/Sensitive Information (SI) to unclassified and range from reachback (Atlantic Intelligence Command (AIC) / Mine Countermeasures Technical Centers) to CJTF and components and extended down to and from individual warriors in the field. The demonstration used MLS network bridges/gateways from US to combined forces provided by other demonstrations. C2 was performed with GCCS and service component GCCS COE compliant C2 systems at the component and CJTF levels. The prototype Joint Counter Mine Application (JCA) (level 6 DII COE compliant in GCCS 2.2) and native applications were used to manage the data at this level. Collaborative planning was executed using web-based newsgroups.

**JW086** - Successfully provided a real-time collaborative planning through the Real-time Collaborative Pre-Strike (RTCPS) segment of the demonstration. RTCPS received imagery from the Atlantic Intelligence Center in real time for analysis by the operator. The voice, whiteboard and text interaction (chat room) capabilities enhanced the planning effort in the preparation of a target plan or a pre-strike briefing. RTCPS allows communication with more experienced intelligence analysts for image analysis and interpretation with this feature. No other MLS challenges were met by this demonstration.

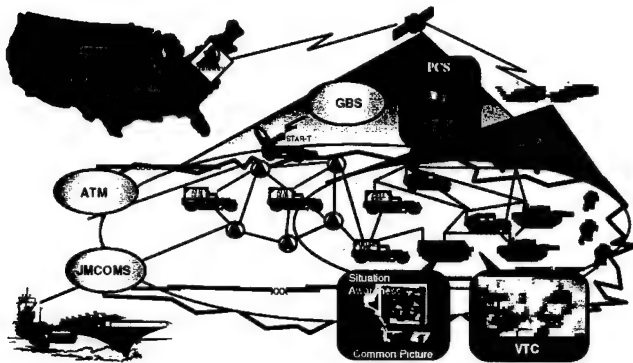
**JW123** - Radiant Mercury (RM) Imagery Guard (RMIG) enabled the real-time dissemination of downgraded imagery across security levels from the SIPRNET to the CWAN. This was done on demand as individual operators on the SIPRNET were able to specify specific images that were to be released to the Coalition. The images were automatically screened for the proper National Imagery Transmission Format (NITF) - Secret (S) header and automatically transferred across the boundary from one network to the lower classification network.

## **Conclusions and Recommendations**

- Several demonstrations included MLS solutions to selected problem areas.
- Some MLS systems were provided with man-in-the-loop sanitization while others demonstrated real automated MLS capabilities.
- Continue work to resolve larger MLS issues.



## Objective 2      *Telecommunications and Information Management Technology that Enhances Data Delivery*



### Objective Statement

- Demonstrate innovative telecommunications and information management technology that enhances data delivery to and from Joint Warriors at the unit level, particularly common operational picture and imagery.

### Technical Challenges

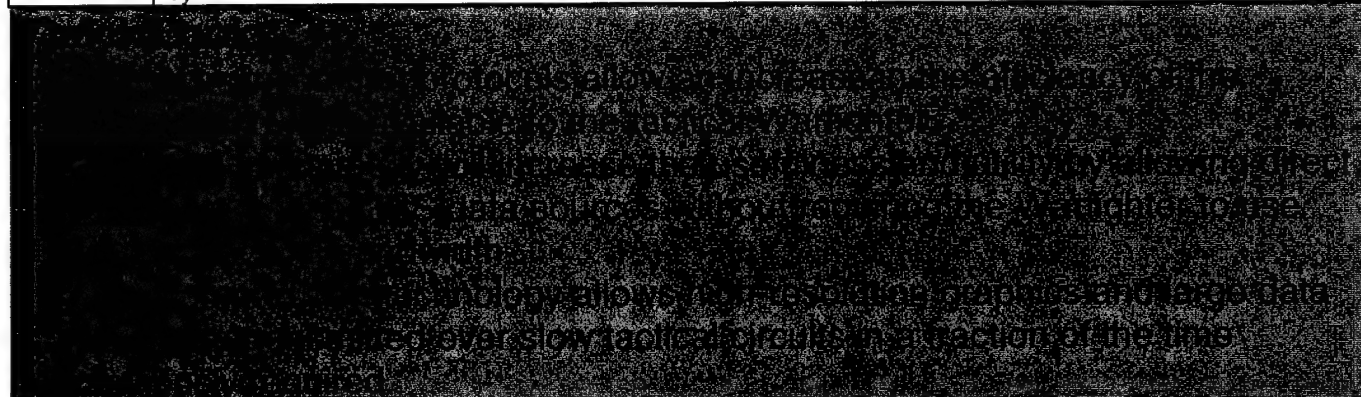
- Demonstrate innovative telecommunications and information management technology that enhances data delivery to and from Joint Warriors to the unit level, particularly COP and imagery.
- New bandwidth enhancements.
- Improved bandwidth enhancements.
- Digital Wide Band Transmission System ship-to-shore communications.
- Defense Information Infrastructure enhancements.

### Results

Demo #	Remarks
JW002	Cellular communications demonstrated in a mobile tactical scenario. Provided Easy-to-Use, fast to setup/takedown, cellular communications for mobile tactical forces.
JW004	Faster and broader availability of encrypted communication.
JW008	Data represented to user in three dimensions.
JW009	Advanced compression techniques for images, to minimize bandwidth requirements. High compression, with resultant good quality, for imagery transmission, facilitating effective bandwidth use and dissemination to low bandwidth users.
JW023	Enhanced delivery of the COP, plans, imagery, etc., via Common Operational Modeling, Planning and Simulation Strategy (COMPASS) integration into GCCS.
JW032	Disseminates real-time data from Global Positioning Satellite (GPS) position location information to theater tactical assets and global C2 nodes via UHF line-of-sight (LOS) and SATCOM.
JW036	Allows unit level user to receive integrated answer from multiple sources via a single query.
JW039	Adapted COTS techniques to tactical challenges, providing enhanced imagery, Video Teleconference (VTC), collaborative planning and data to the unit level.
JW043	Enhanced delivery of situational awareness data, using Transmission Control Protocol (TCP)/IP, between ship and shore.
JW045	Integrated information management, via a Coalition National Imagery and Mapping Agency (NIMA) server, providing a common interface into available intelligence & geospatial data.
JW068	Utility of Global Broadcast System (GBS), Very Small Aperture Terminal (VSAT), and Battlefield Awareness and Data Dissemination (BADD) to support the distributed Air Operations Center (AOC) and mobile JFACC concept.
JW073	Provided an innovative IP-based radio frequency (RF) tactical networking capability to support dissemination of ISR information to the tactical commanders.
JW074	Flexible multimedia communications over SATCOM and LOS paths in the UHF, SHF, EHF and Commercial frequency bands.
JW080	Submarine contributions to collaborative planning, e.g., periscope images and Unmanned Aerial Vehicle (UAV) video and UAV precision targeting data, given higher-bandwidth communications.



JW085	Rapid dissemination of Position Locator Information (PLI) information to tactical users with innovative TCP/IP based networking & communications solutions (Message Data Exchange (MDX)).
JW086	Distributed COP, intelligence, & imagery data using an innovative combination of existing DII, MILSTAR, and GBS comm. Data delivery enhanced by reducing duplicate reporting.
JW089	Used COTS to emulate Theater Deployable Communications (TDC) capabilities available to deploying USAF Component Headquarters (HQs) in late 1998.
JW101	Capability to send COP and imagery data as message attachments, to joint warriors at all levels, with encryption & authentication.
JW112	GBS Reachback via GBS; advantages of future Integrated Broadcast Service; end-user access & dissemination of National primary imagery. Showed an important prototype GBS Reachback capability via a single GBS transponder. Delivered national sensor data via GBS, providing more data more quickly than existing Tactical Related Application (TRAP)/Tactical Receive Equipment (TRE) systems.



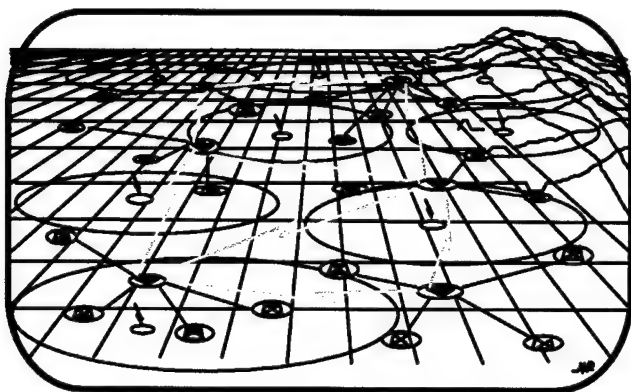
## **Conclusions**

- The rapidly maturing mobile Internet protocol innovations utilizing existing RF systems holds great promise for providing the individual Warrior with enhanced situation awareness (SA).
- The GBS Reachback capability, utilizing existing space assets, is a significant technical breakthrough that will provide a new capability to the deployed Warfighter.
- The demonstrated data compression technology, allowing for significant reductions in transmitted bits, can be deployed today with immediate payoffs to the tactical Warfighter.
- The test JWID network does not represent the bandwidth limitations placed on the tactical/deployed Warfighter. Many demonstrations can only be used effectively in a garrison environment.



## Objective 3

## Dominant Battlespace Awareness



### Objective Statement

- Demonstrate tailorable Dominant Battlespace Awareness (including 3D) in a Coalition Task Force setting, highlighting multi-modal data fusion, Common Operational Picture (COP), and track correlation and management.

### Technical Challenges

- Common Operational Picture needs to address distributed network management and distributed track correlation.
- Demonstrate how technology insertion can provide a fused, near real-time, true representation of the Warrior's battlespace, and the resultant capability to order, respond, and coordinate actions both horizontally and vertically to the degree necessary to prosecute the mission in the battlespace.
- Solve Variable Message Format and Tactical Digital Information Link - J (TADIL-J) data interoperability issues.

### Results

Demo	COP	DBA	Remarks
JW008		●	3D Volumetric provided track data on a display. The display did not show the COP, only representative features. Found to have little utility.
JW032	●		Situational Awareness Beacon with Reply (SABER) provided distributed track correlation on beacon data and provided a fused picture to the COP through Joint Maritime Command Information System (JMCIS).
JW043	●		JACCS provided vector maps to depict terrain detail on the COP. This capability created a real-time COP at workstations distributed across the battlespace.
JW044		●	Battlespace Visualization provided a fused, near real-time, true representation of the Warrior's battlespace. Did not order, respond, and coordinate actions horizontally and vertically.
JW045	●		Imagery and Geospatial (I & G) Support provided images and geospatial data for the COP from the SIPRNET through the C2 Guard.
JW073	●		Joint Countermine provided mine/minefield data for the COP. Fused ISR and force assets. Integrated the use of imagery as well.
JW080	●		Submarine Joint Coalition Combat Ops (SJCCO) provided a synergistic mixture of equipment utilizing all the demonstrations onboard contributing to the COP.
JW085	●		Integrated Situational Awareness (ISA) provided battlespace situational awareness with expanded set of input options, processing tools, retrieval/display/distribution of COP along with ISR and Meteorological and Oceanographic (METOC) segments.
JW086	●		Sensor to Shooter shared information/imagery received from multiple sources with Common Operational Picture through the capabilities in the TBMD/JMCIS segment. Provided dual track correlation of Theater Ballistic Missile (TBM) launches.
NOTE			Technical Challenge #3--Variable Message Format and TADIL-J interoperability issues were not addressed by any of the demonstrations.

## **Conclusions**

Collectively JW032 (SABER), JW043 (JACCS), JW045 (I&G Support), JW073 (Joint Countermine), JW085 (ISA), and JW086 (Sensor-to-Shooter) made significant contributions toward providing a comprehensive Common Operational Picture. Issues remain concerning dual track correlation, symbology, format interoperability, use of the COP with loss of input segments, and general integration and communications/super system management which makes the entire objective a candidate for further in depth assessment. This is a complex issue. Selected Warfighters need to be given the opportunity to learn as much as possible and fully understand the prospective contributing pieces in order to help in the development of a system which provides all aspects of Dominant Battlespace Awareness.

## **Recommendations**

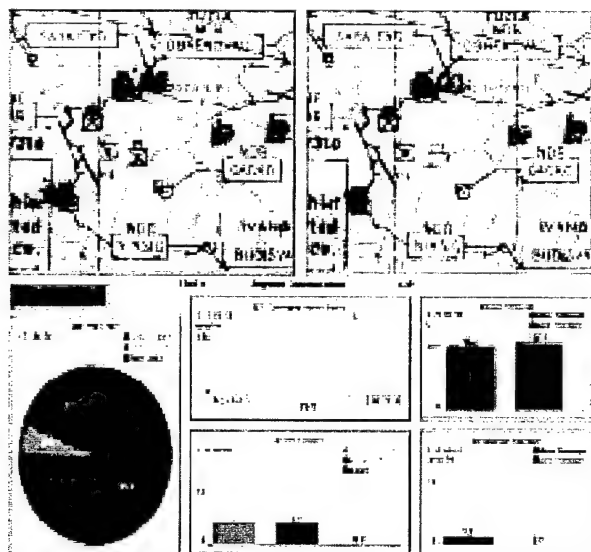
- The technical issues should be further investigated by a technical evaluation organization before any system fielding.
- Train selected Warfighters on current Battlespace Awareness technology to develop experts who can lead and participate in further development and assessments during exercises, lab environments or actual operational tests.

### **Quick Look**

Several demonstrations made significant contributions to the Common Operational Picture. Issues still to be examined involve dual track correlation, symbology, format interoperability, use of the COP with loss of input segments, and general integration and communications/ super system management. Complex objective requiring further investigation and guidance.



## Objective 4 *Sensor to Shooter Technology*



### Objective Statement

- Demonstrate sensor-to-sensor and sensor-to-shooter technologies to enhance combat identification and theater missile defense in a Coalition environment, and to provide targeting information for stand-off and precision guided munitions utilizing selected portions of the JROC approved precision strike C4I architecture.

### Technical Challenges

- Demonstrate the capabilities to share sensors among the Services, process the required targeting information and disseminate the information to selected weapons platforms while simultaneously providing required information to multiple command centers that will coordinate the employment of those weapons in a Joint Engagement Zone.
- Demonstrate sensor-to-shooter technologies that support air-to-air, ground-to-ground, ground-to-air, and air-to-ground that enhance battle management and are interoperable/compliant with the DII COE.

### Results

Demo #	Arch	DII COE	Remarks
JW012	●		Joint Continuous Strike Environment (JCSE) consolidated sensor outputs. Applied results to targeting function. Disseminated target mission messages to Services.
JW028	●		Processed Transporter Erector Launcher (TEL) targeting information not previously available, and provided to AOC personnel for action.
JW032	●	●	SABER provided beacons that enhanced the friendly combat ID function.
JW043	●		Provided a low cost laptop extension to AFATDS that facilitates Distributed Collaborative Planning (DCP) on TMD issues with Components and Allies.
JW045	●		Provided imagery and geospatial data with C2 guard in support of coalition target planning.
JW085	●	●	ISA provided enhanced COP by resource management of sensors.
JW086	●		Provided warning, targeting and sensor cueing data to rapidly plan and execute strikes using missile systems and naval gunfire.
JW112	●	●	Provided reachback capability for requesting imagery and other intelligence data that was then sent over GBS to the requester.

Most of the demonstrations that supported this objective worked to bring different techniques and technologies together to meet the overall sensor to shooter objective. Sensor systems like Tactical Control System (TCS) (JW086) provided the ability to share sensors between services. Naval Surface Fire Support (NSFS) Weapon Control System (NWCS) (JW086) tasked TCS to fly a simulated Predator over specific targets and send the imagery back to various service locations. TCS sent back image stills and TACFILE messages to the NWCS. TCS provided live video to the CCTF 9TV system for direct viewing on board the USS John C. Stennis, and to the Joint Forces Air Component Commander (JFACC) (JW068), including the Speckled Trout aircraft. It also

provided selected payload images to Joint Deployable Intelligence Support System (JDISS) (JW015), JSTARS (JW028), and the submarine intelligence analysts, and sent selected imagery to National Imagery and Mapping Agency (NIMA) for archiving (JW045). Sensor information was also sent directly to COP (JW085) from Theater Ballistic Missile Defense (TBMD) (JW086), Situational Awareness Beacon with Reply (SABER) (JW032), Enhanced Position Location Information System (EPLIS) (JW085), and Tactical Digital Information Links (TADIL-J) and the Enhanced COP (ECOP) provided enhanced management capabilities. Joint Attack Command and Control System (JACCS) (JW043) provided Fire Support data retrieval and input to the NWCS.

Enhanced processing capabilities were demonstrated by Joint Continuous Strike Environment (JCSE) (JW012) which received targeting data from NWCS and COP and provided enhanced capabilities to prioritize targets, match weapons and deconflict air space. Collaborative tools like those provided by Real Time Collaborative Pre-Strike (RTCPS) (JW086) also provided enhanced capabilities to support targeting and coordination.

Enhanced transparent communications support was provided by the GBS Reachback capability (JW112) which provided a means to receive indications and warning data, cross cueing, Primary Imagery Products to Warfare Planners (PRIME) imagery data and other threat and targeting data.

Those demonstrations that were DII COE compliant are annotated in the table. In depth DII COE discussions can be found in the Objective 6 discussion.

## **Conclusions and Recommendations**

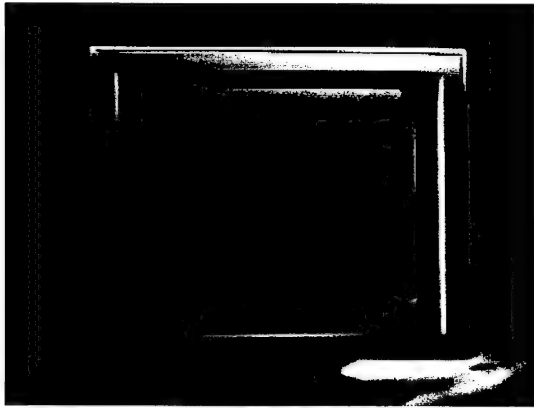
While each demonstration brought part of the solution to meet the sensor to shooter objective, it was in the combination of these demonstrations that the overall architecture was achieved. While it did not cover all of the potential interoperability that could support the warfighter, the synergistic approach provided enhancements to sensor sharing, target and weapon assessment and pairing, and intelligence dissemination. The cooperation and teaming of many of these demonstrations provided a capability to multiply support to the warfighter and should be encouraged in future JWIDS.



**Black Box**  
The synergistic approach provided enhanced sensor to sensor and sensor to shooter capabilities.  
Many of these demonstrations provided a capability to multiply support to the warfighter.  
Enhanced enhancements are required to optimize sensor use and weapon assessment.



## Objective 5 *Enhance & Refine Information Ops/IW*



### Objective Statement

- Demonstrate technologies that enhance information superiority through the use of Information Operations/Information Warfare (IO/IW). These technologies should provide assurance of Coalition access, use, and integrity of Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) systems while preventing unauthorized use of the same.

### Technical Challenges

- The technology should provide Indications and Warning of intrusion/attempted intrusion immediately to the user, as well as pinpointing the source of attack.
- Also needed is a modeling and simulation capability that will enhance Coalition forces' ability to deny an adversary use of his critical information systems and provide measures of effectiveness to evaluate such activity.

### Results

Demo #	Indications & Warning	Modeling & Simulation	Remarks
JW015	•		NetRanger detected intrusion and source of attack.
JW052	•		Analytic capability for determining the nature/extent of intrusions.

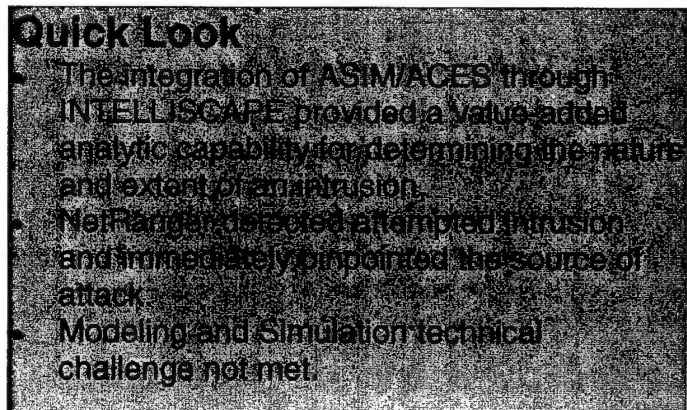
- = Indicates that technical challenge was met

**JW015** - NetRanger, as part of JWID-015, provided Indications and Warning of intrusion/attempted intrusion immediately to the user, as well as pinpointing the source of attack. It also demonstrated the capability for the operator to lock out intrusion attempts in real-time.

**JW052** -The Automated Security Incident Measurement (ASIM) and Automated Computer Examination System (ACES) immediately notified the user of intrusions. Provided analytic capabilities that assisted the operator in determining which areas were attacked and assessing nature and extent of the activity. ACES demonstrated a capability to perform a forensic level examination of the effected system and establish an evidence chain of custody for legal proceeding against intruders. Information Warfare alert messages were disseminated to Coalition forces and the system was able to lock out intrusions on subsequent attempts.

### Conclusions and Recommendations

While the intrusion detection systems demonstrated are all proven systems (versions of ASIM and NetRanger are used by service components and ACES is used by the FBI) they are not normally used by the Warfighters at the JTF level and below. Computer Incident/Emergency Response Teams relied upon to deal with intrusions. These systems demonstrated a level of automation that could provide the Warfighters, at the JTF and below, an organic capability that would enhance information assurance.



## Objective 6 *COTS/GOTS Technology*

### Technical Challenges

- Split-base operations (SBO) to minimize the footprint of equipment and personnel that actually have to deploy into the theater of operations. Send Warriors forward and connect to planners electronically.
- Demonstrate an automated tool that will provide info system and network planning, engineering and management of a joint network across tactical and strategic domains, including: Dynamic bandwidth allocation, Information systems security, Addressable network solutions, Quality and ATM technologies.

### Objective Statement

- Demonstrate the ability of Commercial Off-the-Shelf (COTS)/Government Off-the-Shelf (GOTS) technology to provide constant data exchange with in-garrison, in-transit, and deployed elements of the CTF.

### Results

Demo #	SBO	Auto Tools	Remarks
JW004	•	•	Secure data links over tactical and commercial voice lines that could be used for network planning and operational execution.
JW011	•	•	Cellular phone and mobile nodes worked with local infrastructure (CWAN) and tactical environment (Mobile Subscriber Equipment (MSE) backbone) with long haul backhaul over VSAT to remote locations.
JW015	•	•	Information exchange between SIPRNET, LOCE networks and CWAN subscribers. MLS server capability to conduct collaborative planning and network planning.
JW023	•		A deployable suite of automated planning tools, embedded DCP and Modeling and Simulation (M&S) segments for campaign and mission planning.
JW039	•		Used HS MUX/DEMUX card within MSE backbone to conduct battlefield VTC for collaborative planning.
JW043	•		COTS integration via use of Netscape Web server to exchange info. Allowed non-AFATDS systems to share fire support info.
JW045		•	Provided ATM and Fastlane COTS capabilities.
JW068		•	Provided ATM and Fastlane COTS capabilities.
JW080	•		USS Atlanta's TAC-4/ACOP C2PC provided situational awareness data .
JW085	•		Provided battlespace situational awareness with expanded set of input options, processing tools, retrieval/display/distribution of COP along with ISR and METOC.
JW101	•	•	Secure messaging capability and interoperability with legacy systems with data exchange, multimedia attachment, directory and information management capability.
JW112	•		Use of COTS and GBS software to enable reachback functionality.

### Conclusions and Recommendations

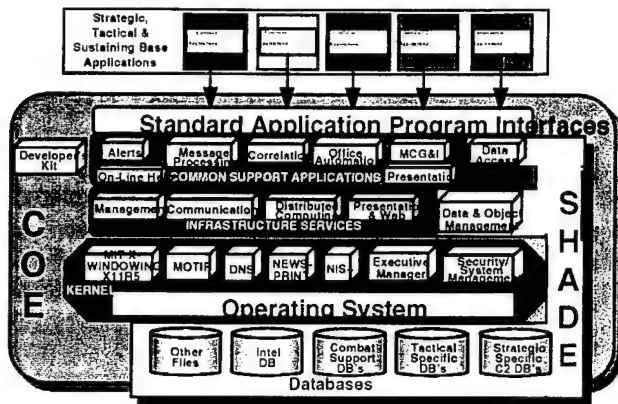
COTS/GOTS solutions provided many of the enhanced capabilities to the warfighter. COTS solutions supported a variety of functional areas that allowed the exchange of data with in-garrison, in-transit, and deployed elements. These solutions proved very useful in the Coalition environment, and several instances of interoperability between nations on different info systems were provided by the use of COTS products. GOTS solutions were integrated on single workstations and provided the warfighter the capability to develop integrated solutions from deployed locations, many times through the use of COTS web technology.





## Objective 7

## DII Common Operational Environment



### Objective Statement

- Demonstrate enhancements to the Defense Information Infrastructure (DII) that improves its utility and interoperability to the CTF.

### Results

Demo	Remarks
JW004	Potential to enhance by restricting access by non-Paralon PathKey (PPK) callers and hanging up on them. This activity is displayed on the administrative workstation.
JW015	DII based JDISS 3.0 UNIX and NT workstations provided a family of interoperable tools for basic intelligence and imagery analysis. Allowed for interoperability and collaboration with GCCS. JDISS MNW allowed operator to push non-formatted intelligence products from the SIPRNET to the CWAN. JDISS Multimedia Collaborative Manager (MCM) segment provided plug-in collaborative planning and VTC enhancement for DII based UNIX systems.
JW023	Enhanced utility of the DII by enabling warfighters to conduct operational planning with non-DII legacy systems, to access and collaboratively share plans, and to share products and information to/from DII-Compliant C4I systems. COMPASS is DII COE Level 5 compliant.
JW032	SABER interoperated directly with the JW085 as well as JMCIS and USMC 3.0 versions. As JMCIS moves to full GCCS DII COE compliance, the SABER segment will also maintain compliance. SABER's direct feed to JMCIS/GCCS will make SABER interoperable with all Services and Allied forces.
JW068	Demonstrated enhanced collaborative tools and information management which will enable further evolution of the DII COE as a core infrastructure for DOD information systems.
JW073	Built on top of the DII COE and provided additional countermines functionality. Showed the ability to communicate via the CWAN using the RM server, and validated the JMCIS to NT PC process. Enhanced war planning operations by providing access to various imagery, intelligence, and other information displayed by the Netscape browser, a client of the NT PC architecture.
JW074	Mini DAMA provided increased bandwidth to submarines from 16 to 38.4 Kbps using new wave form. Challenge Athena provided enhanced throughput with SHF SATCOM by increase of receives only 368 Kbps to full duplex 1.44Mbps. TGAN provided X.400 messaging service to MNTG. The increases in bandwidth and X.400 features provided a significant increase in capability.
JW085	The enhanced COP tools and the EPLIS are COE/DII compliant.
JW101	DMS is an element of DII at level 3 compliance.
JW112	Demonstration of enhancements to the DII that improved its utility and interoperability to the CTF by the near-term Integrated Broadcast Service Concept (IBS-C) and Reachback functionality extension and utility of the GBS element of the Defense Information System Network (DISN)/DII.

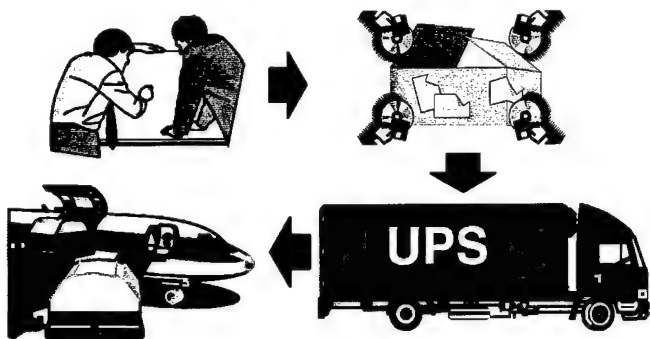
### Conclusions and Recommendations

- As communications methods continue to become DII compliant, interoperability between the services will enhance collaborative planning for the Joint Warfighter.
- Recommend all services continue to move forward with DII compliance.



## Objective 8

## Integrated Logistical Support



### Objective Statement

- Demonstrate an integrated, near real-time focused logistics system with a planning and decision support capability. The system will track all classes of supply, pre-positioned war reserve assets, and personnel, to and from the sustaining base and wholesale depots.

JW106 - Global Combat Support System (GCSS) - provided an integrated, near real-time, logistics focused capability with planning and decision support tools from the Integrated Consumable Item Support (ICIS) model and selected applications from the Logistics Anchor Desk (LAD). GCSS combined the ability to track all classes of supply, prepositioned war reserves, and personnel to and from the sustaining base and wholesale depots and home station through the incorporation of Joint Total Asset Visibility (JTAV) and Joint Personnel Asset Visibility (JPAV) applications. Additional applications beyond those specified in the plan were demonstrated. These included: Global Transportation Network (GTN), Joint Computer-Aided Acquisition and Logistics Support System (JCALS), Joint Engineering Data Management Information and Control System (JEDMICS), Knowledge-Based Logistics Planning System (KBLPS), and TRANSCOM Regulating and C2 Evacuation System (TRAC2ES).

### Results

Applications	Description
ICIS	Combines common critical items throughout DOD. Provides query on demand and automatically apportions available assets among all users into one database.
GTN	Used to track the identity, status, and location of cargo and passengers from origin to destinations.
JPAV	Provides personnel information for warfighters deploying into, operating within and departing from an AOR.
TRAC2ES	Combined transportation, logistics and clinical decision elements into a seamless patient movement and location information system.
CVW	Provided a VTC and whiteboard capability for logistical planning with other organizations.
ELB	Provided multiple applications to enter data into one event log for historical /planning purposes.
JTAV	Provided access to timely, accurate information on the location, movement, status and identity of units, personnel, equipment and supply and provided access to decision support tools.
JCALs	Provided a flexible architecture to share data in a distributed environment across sites, organizations, and legacy systems.
JEDMICS	Used digital techniques to store, retrieve, reproduce and distribute engineering drawings and related technical data.

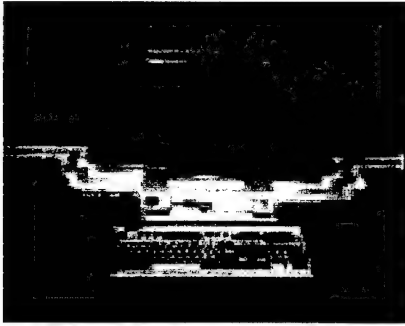
### Conclusions and Recommendations

- JW106 made a major contribution to solving the requirements associated with this objective.
- Not all required connectivity between applications was available, and there were human factor issues that need to be resolved before this system can provide a totally integrated logistics solution.

### Quick Look

- JW106 made a major contribution to solving logistics requirements and integrating GOTS logistics systems

## Objective 9 *Integrated Single Computer Operations*



### Objective Statement

- Demonstrate the ability to provide an integrated solution for all tactical and non-tactical applications on a single computer.

### Technical Challenges

- Demonstrate the ability to provide all tactical applications on a single computer.
- Demonstrate the ability to provide a common non-tactical environment.

### Results

DEMO #	Single Computer	Common Environment	Remarks
JW015	•	•	Provided intelligent support on a single computer.
JW085	•	•	Applications integrated together resided on separate computer systems, but could be hosted on a single system.
JW101	•	•	Provided messaging capabilities on host computer with other applications.
JW106	•	•	Provided logistics support on a single computer.

- = Indicates that technical challenge was met

**JW015** - DII-based Joint Deployable Intelligence Support System (JDISS) provided an integrated family of plug-in intelligence support and multimedia collaborative software segments based on DII COE, and COTS Multi Level Security (MLS) and Trusted Web technology on a single workstation. JDISS allowed the secure exchange of intelligence data and multi-security level access to web-based products and data. All applications were provided on both NT and UNIX platforms, except the Multi Network Workstation (MNW) was not available on the NT JDISS terminal. It also provided non-tactical applications on these workstations as well.

**JW085** - The use of the C2PC to receive the common operational picture (COP) demonstrated significant use of PC technology for command and control. The C2PC software allowed integration of tactical and non-tactical applications on a single PC. The ISR data (ISRD) architecture was based upon a PC client and an ISR server. The ISR server allowed for transfer of data using net browser http calls.

**JW101** - DMS co-hosted user agent components on the same platform as other tactical applications.

**JW106** - GCSS provided an integrated logistics solution on a single platform. It provided access to multiple logistics applications including ICIS, JPAV, GTN, JCALS, JEDMICS, KBLPS, and TRAC2ES.

### Conclusions and Recommendations

- Intelligence, COP, and logistics integrated solutions provided to the warfighter yielded greater accessibility to required information in functional areas. DMS provided a messaging solution that would reside on a warfighters local workstation.
- Continue integration efforts.

### Quick Look

JDISS, C2PC, DMS, and GCSS provided good examples of the ability to provide all applications in a functional area on a single computer.

# Objective 10

Year 2000



## Objective Statement

- Demonstrate the ability of Information Technology to identify and solve millennial problems in order to operate beyond the year 2000.

## Technical Challenges

- Set system clocks past the year 2000 (Y2K).
- Demonstrate fixes to existing millennial problems.

## Results

Demo #	Jan 1 2000	Feb 29 2000	Jan 1 2001	Remarks
JW004	Pass	?	?	Only assessed on 1 Jan, 2000.
JW015	?	?	?	Software license expired in August 1997.
JW023	Pass	Fail	Fail	COMPASS machines failed to reboot on leap year test; locked up when transitioning to year 2001.
JW032	Pass	Pass	Pass	SABER tracks updated properly.
JW036	Pass	Pass	Pass	Report by program manager. See Solaris 2.5 results below.
JW039	Pass	Pass	Pass	No problem indications.
JW043	Pass	Pass	Pass	No problem indications.
JW044	Pass	Pass	Pass	No problem indications.
JW045	Fail	?	?	NIMA servers locked up when transitioning to Y2K.
JW052	Pass	Pass	Pass	No problem indications.
JW060	?	?	?	Only checked the operation of the JWID Clock. No report on the actual data base operating system time being changed.
JW068	Pass (Barksdale) Fail (Stennis)	?	?	Version 4.1.x of SUN Operating System (OS) used with Deployable AOC (DAOC) Advanced Planning System (APS) will not allow system admin to manually set the system date to the year 2000. If the system date is set to year 31 Dec 1999, it will advance to year 2000 correctly and DAOC APS appears to function without error. DAOC-FLEX Y2K errors could not be attributed directly to the Y2K issue due to FLEX software problems at that time.
JW073	Pass	Pass	Pass	Only reported on Stennis. No indications of Y2K problem. See also HP UNIX 9.0.7 results below.
JW074	Pass	Pass	Pass	No problem indications. Multi-cast applications (JMCIS PAD and CHAT) worked. Timeplex not tested.
JW080	Pass	Pass	Pass	No problem indications.
JW085	Pass	Pass	Pass	No problem indications. See also HP UNIX 10.20 results below.
JW086	Pass	Pass	Pass	JSTARS, RTCPS, and TCS terminals on Stennis only report received; No problem indications.
JW101	Pass	Pass	Pass	Fortezza certificates expired.
JW106	Pass	Pass	Pass	Tested clients only since GCSS was using existing databases on the NIPRNET.
JW112	Pass	Fail	Pass	PRIME and IBS-C portions did not recognize Y2K as a leap year.
JW123	Fail	?	?	One of three required processes failed to recognize the audit file. Unknown if this is a Y2K issue or software glitch.

- Demonstrations 002, 008, 009, 011, 012, 028, 036, and 089 did not participate in Y2K assessment.
- Testing was also performed on various operating systems and results are provided below.

Operating System	Jan 1, 2000	Feb 29, 2000	Jan 1, 2001	Notes
Solaris 2.5.1 Operating system	Pass	Pass	Pass	No problem indications. Noted, that years past 2069 were not recognized and base year (when 00 was entered as year only vice 2000) was 1970.
GCCS 2.2	Failed 1 site Passed 1 site	?	?	GCCS 2.2 (Solaris 2.3) locked up when clock rolled over to Jan 1, 2000. Rebooting system to 1997 found that all user accounts had been lost. Failure occurred aboard USS Nassau, system passed at Fort Gordon site.
HP UNIX 9.0.7 (JMCIS 2.2)	Pass	Pass	Pass	No problem indications.
HP UNIX 10.20	Pass	Pass	Pass	No problem indications.
SunOS 5.3	Pass	Fail	Fail	Leap year problem: Upon reboot saw message "TOD clock not initialized - Check Date". Date returned to 1970. 2001 problem: machine froze when date changed.
Windows NT	Pass	Pass	Pass	No problem indications.
Exchange 4.0 Email	No test	No test	No test	Known to not be Y2K compliant.



There were no demonstrations in JWID 97 that met the technical challenge of demonstrating the capability to fix existing millennial.

The Y2K assessment was simplistic, performed by the demonstrators themselves. While it does not indicate certification of compliance, it does provide an indication of potential success or problem in the year 2000. Demonstrations that failed to work during this assessment should be further evaluated because of the many variables that were not considered in the assessment. Thorough testing of all processes in the software or analysis of how the code handles dates is necessary to determine the full ability to operate after year 2000.

## **Conclusions**

Almost half of the demonstrations had success in meeting the Y2K challenge. Problems included system lock ups and failure to recognize the leap year. Many of the failures were on Sun platforms and Sun has indicated the next release of Sun Solaris should fix this problem. Many demonstrations chose not to participate in the test.

## **Quick Look**

- No demonstrations met the technical challenge to demonstrate fixes to existing millennial problems.
- Almost half of the demonstrations had success in meeting the Y2K date change.
- Many demonstrations chose not to participate in the test.

---

## ***2.2 SPECIAL INTEREST AREA RESULTS***

---



**Special Interest Area** *Coalition Wide Area Network*  
(*CWAN*)

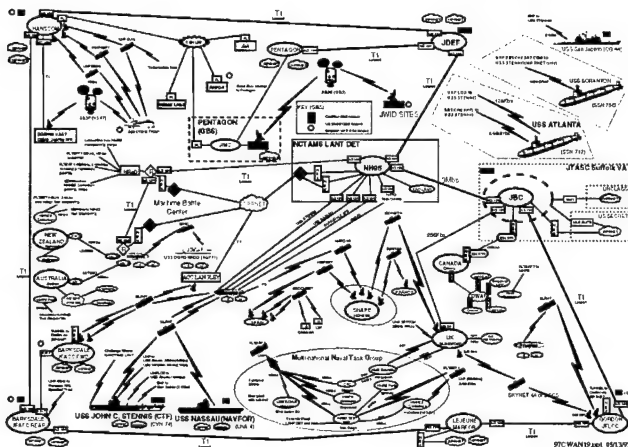


Figure 2-1 Coalition wide Area Network

## Issue

- How was the Coalition Wide Area Network used to support both US and Allied participants during the JWID 97 execution?

## Technical Challenges and Description

In previous JWDs, all US sponsored demonstrations were connected to the US only SIPRNET. This prevented real-time collaborative planning and execution by all Coalition Forces. In JWID 97, the intent was to present all demonstrations on a Coalition Wide Area Network that would allow all Coalition Forces access to all demonstrations. This CWAN was the primary communications means for traffic between JWID 97 sites, including numerous land-based US sites, US ships, airborne Speckled Trout, and several Allied sites and was established to interconnect all sites, US and Allied, as peers, with no multi-level security (MLS) separation. The CWAN consisted in large part of encrypted, leased commercial terrestrial bandwidth - mostly T1 links - and Government or leased satellite bandwidth, typically connecting IP routers at the sites. It included the use of Global Broadcast Service (GBS) for broadcast transmissions to many of the US sites. A back-up capability was provided, via the SIPRNET, for some of the leased assets, with the use of Network Encryption System devices to allow tunneling of Coalition information through more restrictive (i.e., US only) DISN networks.

## Results

The complete CWAN was fully available at the start of the JWID exercise period. Most warfighters reported that the CWAN was available at all times during JWID execution. Coalition Communications Control Center (CCCC) network monitoring results, collected at the JBC site, also substantiated this. Some outages were reported, but were quickly fixed. For example, there was an outage of the T1 leased line between Naval Research and Development Laboratory (NRA&D), San Diego, CA, and the NH95 building at Norfolk caused by a cable cut. The link was restored by the commercial carrier within the 4 hour restoral time. During this outage, all sites that connected to CWAN via NRA&D were isolated from the rest of the network. A back-up for this link, via SIPRNET tunneling using Network Encryption System (NES) devices, was not yet operational at the time of this outage.

Crypto synchronization problems and bad weather-related outages (e.g., power down during thunderstorms), occasionally affected links at the Barksdale, Camp LeJeune, and Fort Gordon sites. The CWAN topology allowed for alternate paths from most land-based US sites, to minimize the impact of any one outage. However, such redundancy was not available for all sites and afloat units would be isolated if their individual links were temporarily unavailable. Confusion over the assignment of IP addresses to the USS Atlanta and USS Nassau also caused communication problems that lasted into the first few days of the exercise period.

Traffic loading and bandwidth utilization statistics were continuously collected by the CCCC during JWID for the 17 main CWAN router-to-router links. The total daytime traffic load (0700 to 1900 hrs, EDT) on the CWAN links, for the 10 working days of the scenario, ranged from approximately 10 Gigabytes to 14 Gigabytes per day. On average, over the entire daytime periods, link loading was only 6 percent of the entire available bandwidth.

Statistics indicated that the bandwidth most often stressed was the 384 Kbps provided to the CJTF located on the USS John C. Stennis, where the majority of the demonstrations were hosted. Its wide-area network linkage was significantly more constrained than that provided to most US land-based sites, typically with one or more T1 links. The statistics show that the 384 Kbps link, carrying traffic inbound to the USS John C. Stennis, had several 5-minute periods of over 90 percent utilization during 8 of the 10 JWID workdays. On 7 of the 10 days, the inbound USS John C. Stennis link was at or above 50 percent utilization for at least 30 percent of the workday. On 21 July, this link was heavily used for the majority of the day, being above 50 percent utilization in 65 percent of the workday utilization samples, and above 60 percent utilization for about 38 percent of the workday. It is likely that 5-minute averages of even 50 -60 percent utilization include smaller periods of time in which the link was congested, with increased delays to end-users.

Other CWAN links of relatively lower bandwidth also experienced periods of congestion although less often than the USS John C. Stennis link. These included: New Zealand-to-Wahiawa (128 Kbps); Wahiawa-to-Australia (256 Kbps); USS Nassau-to-NH95 (256 Kbps); and Barksdale-to-NH95 (512 Kbps). There were a few instances in which the T1 link from NRaD-to-NH95 (Norfolk) and the T1 link from NH95-to-DISA Joint Demonstration Evaluation Facility (JDEF), Arlington, VA link reached utilization of over 90 percent.

**Coalition Communications Command Center (CCCC) Network Monitoring Tools** - JWID 97 included advances in the network monitoring applied to the primary wide-area network. The primary network management tools used at the CCCC included HP Openview, Concord Network Health, and the JDIICS-D application. The information collected and displayed by these tools was easily viewable by any party who had access to a web browser on the CWAN. HP Openview provided the main display of the up/down status of the CWAN links and routers. This display was also available in real-time to non-CCCC at all CWAN sites, via an easy-to-access homepage. Concord Network Health was used to generate reports and graphs from Simple Network Management Protocol (SNMP)-collected CWAN performance statistics, such as link (interface) loading, error rates, missed polls, and packet discards. Daily reports were produced summarizing traffic volume and link utilizations, and highlighting links that merited close watching. Non-CCCC personnel could also connect to the CCCC server for display of some of the Net Health generated graphs and reports.

JDIICS-D was operational at the CCCC, at the JDEF, and the Pentagon site. It also maintained the status of the CWAN and provided this view to the Pentagon and JDEF sites. The JDIICS-D suite of COTS tools included HP NetMetrix, which allowed some real-time detailed examination of any broadcast traffic captured by the NetMetrix probes on the CWAN. This capability was not fully exercised. The Remedy Trouble Ticket system was not used during the CWAN's active network management. JDIICS-D demonstrated its capability for automatic trouble ticket generation, when certain thresholds (e.g., down time) were exceeded.

## **Conclusions**

The CWAN proved itself to be one of the major successes of JWID 97. The link bandwidth provided by the CWAN was sufficient, with the exception of the 384 Kbps link to the CJTF aboard the USS John C. Stennis. This network provided an available and reliable means of communication among the Coalition sites, with sufficient bandwidth available to permit the demonstrations to exhibit all their capabilities. Virtually every site highlighted the CWAN, for providing an excellent infrastructure.

## **Recommendations**

- CWAN is the only way to fully achieve collaborative planning within a Coalition.
- Develop and use architecture for all future coalition exercises and operations.

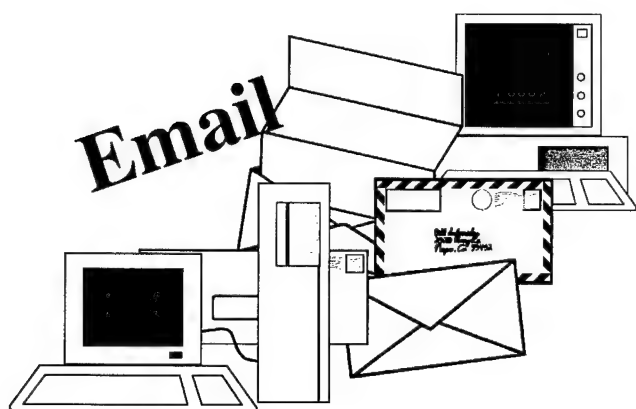
## **Quick Look**

- The CWAN represented significantly different concepts from those used in previous JWIDs.
- Successfully provided peer level network and was well received by the Coalition warfighters.
- Bandwidth provided was more than sufficient for the intersite Coalition traffic, with the exception of constraining bandwidth to the CJTF



## Special Interest Area *Electronic Mail (Email)*

---



### Issue

- How was email used to distribute operational and Master Scenario Events List (MSEL) messages to the Coalition?

### Results

The email service for the JWID Coalition, provided via COTS software and hardware, was successful. The first week of JWID included significant problems with email service to the participants. During the first 3-4 days, users at some sites found they could not successfully connect to their email server to check their mail. Timely delivery of important MSEL information was not being achieved. Administrative procedures were established to resolve these problems and email service improved. The CCCC reported that the unusual large volume and flow of email led to detection of issues concerning the software and hardware that had been selected for this email service. These technical issues, as well as the dominant procedural ones, merit attention in future uses of commercial (COTS) products for JWID or actual JTF or CJTF email.

The original JWID expectation was that the email servers and selected email commercial software would provide for 3 types of email addressees: a) individuals, b) functional (e.g., JW112), c) organizational (e.g., Commander, USS John C. Stennis). The latter would emulate formal messaging, such as AUTODIN. However, as JWID got underway, the organizational mail accounts, that had been established, did not include all that were necessary to reflect the proper C2 structure. In particular, organizational accounts had not been specifically defined nor established for the distribution of the important MSEL messages. The fallback at the start of JWID, to ensure all concerned parties received these, was to use the individual or personal accounts. There were approximately 480 of these, and messages requiring widespread distribution were thus sent to hundreds of addressees. To add to this burden, these early MSEL messages were typically sent with Return Receipt desired, which generates more messages for each mail server to process. Furthermore, the content of the MSEL messages was initially sent as an attachment, in Word97 format, to an email message. This method results in much larger messages, by one or more orders of magnitude, (e.g., up to one Megabyte MSEL messages) as contrasted with the same textual content simply incorporated in the email text. User dissatisfaction was further compounded by the inability of all intended recipients to read Word97 format files, either from having just earlier versions of MS Word or from being on UNIX platforms. Addresses which resulted in delivery problems (e.g., no such account found on the destination mail host) might result in repeated attempts by the sending system to deliver that message. An additional factor was the location of the CJTF, with the majority of JWID demos, on board the Stennis, which had relatively small bandwidth (384 Kbps) for its CWAN link. As noted in the CWAN Assessment summary, at times, this bandwidth was subject to very high utilization. The large volume of email no doubt contributed significantly to this load, and email delivery to the Stennis may have been further delayed during periods of link congestion.

The impact of the above compounding events resulted in serious dissatisfaction with the email service during the first 3-4 days of JWID. Some mail servers were overwhelmed by the volume of work, and in turn would not allow users to connect to retrieve their mail. Most noticeable was the failure of timely delivery of the MSEL messages.

Meanwhile more and more messages were accumulated on the mail servers, awaiting user retrieval by users who could not or perhaps were not even trying to use their established accounts.

Several steps rectified these problems:

- Establishment of appropriate organizational accounts for the distribution of MSEL information; 18 separate addresses were found to be sufficient for MSEL distribution.
- Incorporation of the MSEL information into the body of the email, not as an MS Word97 attachment.
- Definition and distribution of SOPs for JWID email, to include not requesting Return Receipt and other steps to keep mail server load within bounds.



By the end of the first week of JWID, email service was operating well. (To verify this, the CCCC proceeded to send daily sample emails to all sites, which would be resent back to itself, with the time-to-return recorded. In most cases, reflected email was received back in well under one minute from time of sending the original message.) A few users reported dissatisfaction with the email service because of continuing administrative issues including not being made aware of the email service and incomplete or erroneous addresses within the email system.

On the technical side, the experiences of the first few days uncovered potentially serious limitations in the COTS software and hardware that had been selected to support JWID email. These remain as issues to consider, and further investigate, for future selections of software and hardware for email support.

These issues and observations include:

- The selected email software, MetaInfo's Sendmail, had the merits of being both easy to configure and inexpensive. However, it apparently is not optimized for Windows NT. It was noted that, when using the POP3 email standards with MetaInfo on a Windows NT computer, the processor quickly reached nearly 100% utilization.
- Other hardware, such as more robust PCs and UNIX workstations have been shown to provide better access for multiple, simultaneous users. The PCs, used as email hosts for JWID, were sufficient as personal workstations, but possibly under-configured in terms of RAM, processor speed, hard drive interface, and disk space to provide high volume email service.

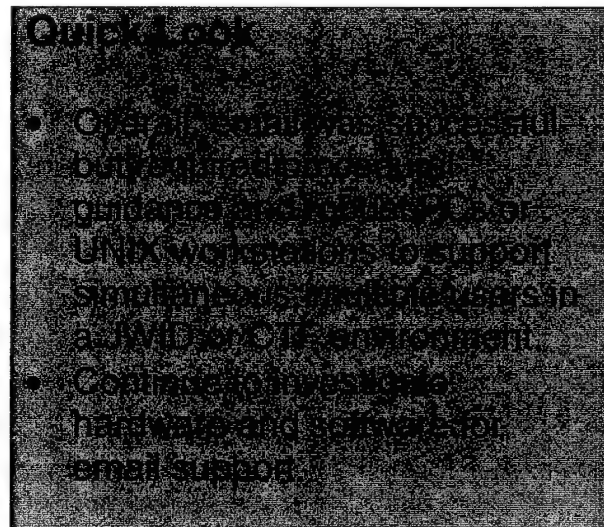
## **Conclusion**

Email provided a viable method for replicating official message traffic but needs further development.

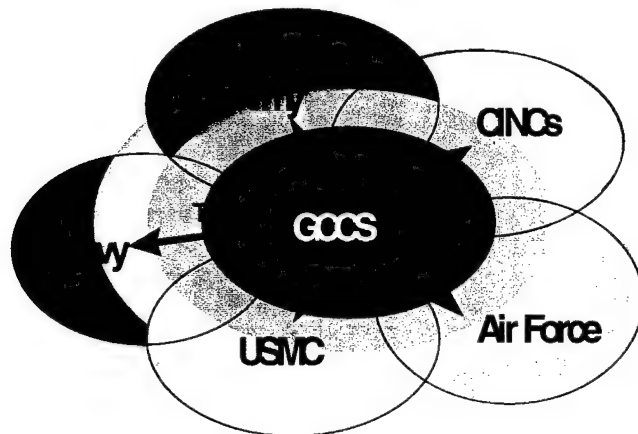
## **Recommendations**

To ensure satisfactory email service in a JWID, or CJTF, environment:

- Define and implement organizational accounts that reflect appropriate C2 structure to emulate official messaging.
- Publish and exercise SOP to minimize sending and processing of unnecessary large message traffic.
- Further investigate, test, and determine what COTS software and hardware are best for e-mail support.



# Special Interest Area *Global Command and Control System (GCCS)*



## Issue

- How did JWID demonstrations integrate and interoperate with the Global Command and Control System (GCCS)?

## Results

Demo #	Demonstration Title	Remarks
JW008	3-D Volumetric Display System	GCCS provided COP track data. There was a lack of training for translation of Link 16 format and control of data to NRaD for translation.
JW015	DII Based Joint Deployable Intelligence Support System	As a DII COE 3.1 workstation, provided a multi-level security platform for collaborative planning and distribution of intelligence information.
JW023	M&S to C4I in the DII COE Warfighting Environment	Provided timely and coordinated data. COMPASS provided info to GCCS for map overlay. GCCS desktop has some redundant icons.
JW032	Situational Awareness Beacon with Reply (SABER)	GCCS passed simulated and actual Global Positioning System location and track data to the Common Operational Picture (COP).
JW036	Sensor Box-Intelligence Support to the Warfighter	Sensor Box was accessible via a GCCS platform. GCCS provided web access to mission planning tools (e.g. CTAPS).
JW043	Joint Attack Command & Control System	GCCS provided interface to mission planning tools (e.g. JMCIS). Unit positions not automatically fed from GCCS.
JW044	3-D Battlespace Visualization	GCCS provided track data to the demonstration. All GCCS tracks were displayed and operational displays are reliable. The demonstration provided its own query function which was different than the query function found on GCCS.
JW060	Trusted Coalition Scenario Database	GCCS exchanged coalition secret and releasable US Only data between coalition partners.
JW068	Deployable Distributed JFACC with Airborne Command Cell	GCCS exchanged distributed, collaborative air planning and mission execution monitoring, and situational data to and from coalition partners. The combination of FLEX, WFA, CVW, JPT, GCCS, APS and DSS platforms resulted in a good picture of the battlefield, allowing all players to view the same picture providing real-time feeds and updates.
JW073	Joint Countermine C4ISR	GCCS provided a DII COE platform for prototype countermine C4ISR segment.
JW085	Integrated Situational Awareness	GCCS provided a DII COE platform for collection, processing, retrieval, display, mission planning, and distribution of COP data, including TADIL-J management, meteorological, and space data, for its own demonstration as well as the source of COP data for other demonstrations. ISA has some excellent enhancements for the GCCS environment, especially PC based GCCS users.
JW086	Joint Sensor-to-Shooter for TMD & Rapid Strike	GCCS provided a DII COE platform for passing ballistic missile launcher warning, targeting, and sensor cueing data to coalition forces, including distribution of COP data.
JW101	Defense Message System for the Warfighter	GCCS provided a DII COE platform for secure message handling within and between US and coalition forces.
JW106	Global Command Support System	Demo had no interface with GCCS. JPAV as a client-server application was not integrated with other Windows-based GCCS applications. A JOPES database display via the COP has potential.
JW123	Radiant Mercury Imagery Guard	GCCS provided a DII COE HP (TAC3/4) platform for the exchange of multi-level classified imagery within and between US and coalition forces for collaborative planning.
Allies	Canadian National Headquarters, New Zealand Defence Force, Australian Defence Force, United Kingdom COP Dissemination and Support	Exchanged track and intelligence data, and conducted coalition collaborative planning activities via GCCS.

GCCS provided DII COE platforms for many demonstration applications and C4ISR data exchange between echelons and coalition partners. Minor problems and issues that warrant further review and action include:

- The Data Collection system had to be rebuilt from scratch, i.e. by trial and error, to transition it from standalone to a client environment. There were no checklists to perform these transitions.
- The JACCS problems with manual only ground feeds from GCCS/COP are being worked at the individual service level (Army and Marines).
- The 3-D Battlespace Visualization, JW044, used a separate, less powerful query than GCCS. Their analysis of the competing query systems reinforces the need for a standardized query system.
- GCSS (JW106) did not have connectivity with GCCS.
- General support tools provided by GCCS are different than those normally used by the individual demonstrations and are not being well received, e.g. , Applixware, collaborative planning tools, whiteboards, teleconferencing.
- Redundant desktop icons wasted space.



## Conclusions

GCCS overall performed well and provided a centralized workstation to integrate information required by the Warfighter. The major issue that is being addressed by GCCS program manager is the automation of ground track feeds to support near real-time COP information. With service solutions as far away as three years, e.g., the Army Battle Control System, an interim fix is needed. As a general support capability, standardized systems such as query systems and standard support applications, is a must for operational performance optimization and joint training, as well as technical interoperability.

## Recommendations

- Automate the ground track feeds.
- Build a checklist for converting GCCS servers to a client environment.
- Review the Graphical User Interface (GUI) for space saving opportunities.
- Highlight query system standardization to systems entering DII COE certification to sponsors.
- Place more emphasis on a thorough, more rapid process to select definitive general support tools.

## Quick Look

- GCCS overall performed very well with no major problems.
- Provided a centralized workstation to integrate info required by Warfighter.
- Limitations included:
  - Manual ground feeds
  - No GCSS - GCCS connectivity
  - Not compatible tool sets

(This page intentionally left blank)

---

---

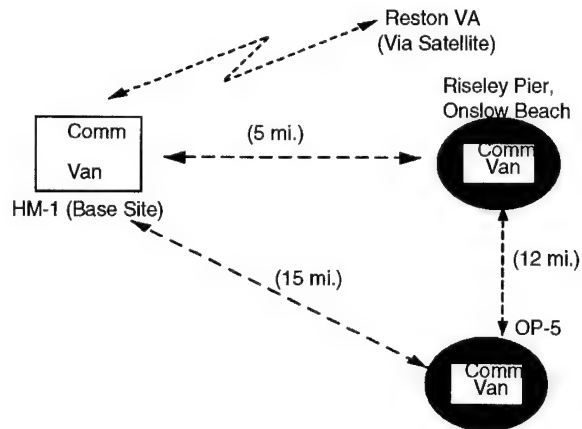
### ***2.3 DEMONSTRATION ASSESSMENTS***

---

---

# **JW-002 *Mobile Expeditionary Cellular Communications Site (MECCS)***

**Sponsor:** Capt Warren Ide, USN, N61 (703) 604-7807, email: Ide.Warren@hq.secnave.navy.mil



## **Description**

- Mobile encrypted cellular tactical communications system.
- Worldwide connectivity via the Public Switch Network using portable VSAT satellite system to facilitate voice, VTC, email, internet, application sharing, whiteboard and image transfer capability.

## **Capability Assessment**

- Full duplex voice and data (128Kbps) exchanges can be accomplished between cell units and public switch subscribers worldwide.
- Provided communications compatible with both commercial and government (DSN) networks.
- Provided a mobile MECCS Base Station to operate up to 15 cellular hand sets and Satellite Communications Package from a transportable High Mobility Multipurpose Wheeled Vehicle (HMMWV).

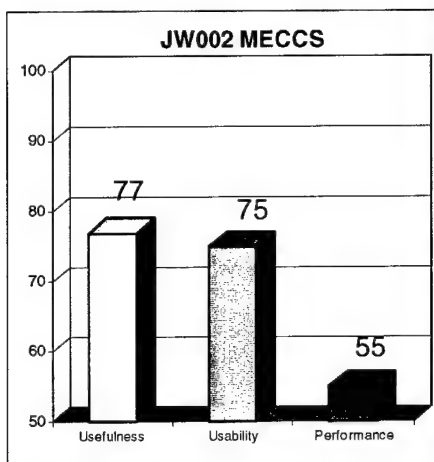
## **Objectives Supported**

Objectives 2, 4, and 8 - Provided local cell-to-cell voice capability, both secure and non-secure. Provided cell to/through remote site connection for access to the worldwide telephone system (comm van, both military and commercial). Provided mobile site to remote site connectivity for exchange of email (at 128 Kbps) and full Internet access. Provided video teleconferencing from site to remote site and from site through remote site to worldwide locations. Included Liveshare software to allow collaborative planning and applications sharing.

Objective 5 - Provided two levels of encryption (end-to-end encryption, using the SKIPJACK slices, and link encryption, using the site KIV-7[KG-84/PC]). Also demonstrated link to ATT-3600 (Industry equivalent to STU-III) at the remote site.

Objective 6 - System breakdown, relocation and set up accomplished in approximately two hours. One re-deployment mobile cell-to-cell communications was maintained using organic battery power. Users also demonstrated the capability to use the cell-to-cell capability under all conditions with access to the Internet, email and VTC in garrison or deployed locations.





## Quick Look

- MECCS provided a quick deployment COTS capability that could be immediately fielded with add on components of cell crypto, VTC, satellite communications with worldwide telephone access available separately or in any combination as required by the mission.
- MECCS provides a plug and play capability that can be modernized as new technology becomes available.

## Results

**Usefulness – 77%:** Encrypted cell (cell-to-cell, in clear text and use of SKIPJACK slice) allowed real-time information exchange (voice, data, email, VTC) both locally and to worldwide locations.

**Usability – 75%:** Plug and play operation user friendly with both commercial and government (DSN) systems. Information transfer was consistent up to 2-3 miles in wooded areas and 3-5 miles in open space and over water. VTC audio and video consistency allowed operators to effectively discuss operational issues and conduct collaborative planning.

**Performance – 55%:** The availability of the system was almost 100%. The requirement to tear-down, relocate and set-up took a range of time from 15 minutes to over 2 hours. Delays were experienced in getting the satellite realigned or reconnected via a commercial carrier after each move to another location.

## Value Added

MECCS provided COTS hardware and software to maximize the tactical advantage of encrypted cellular communications and cellular personal computing stations with a range of un-encrypted and encrypted communications for garrison, enroute and deployed locations. Quick connect and disconnect of the encryption device provided additional security for tactical exit situations where compromise of equipment and security applications must be evacuated or recovered for later use.

## Conclusions

MECCS proved to be a tactically efficient system that benefited the Warfighter by providing an innovative new and different methods of communication with state of the art cell, VTC and network equipment to support expeditionary communications.

## Recommendations

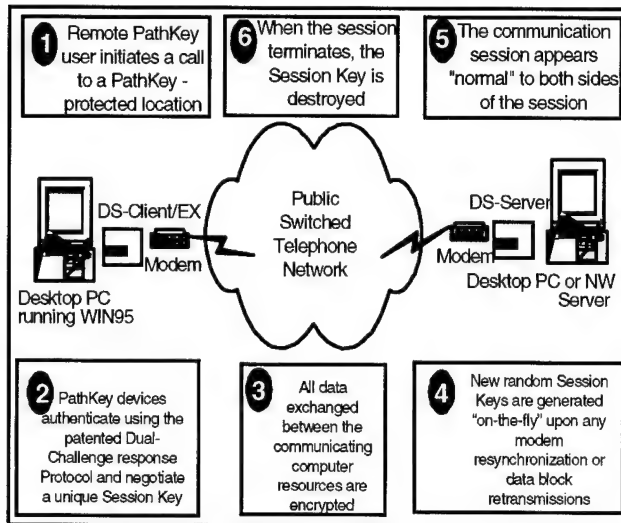
- Technology has proven capability and should be ready for immediate employment from highest command levels down to unit level for strategic and/or tactical situations.
- Identified additional capabilities and add-ons during follow-on development should enhance MECCS operations.

## Warfighter Impressions

- MECCS technology allowed the warfighter to conduct mobile voice, Internet and VTC to both CONUS and overseas locations.
- Despite having to relocate frequently, warfighters readily accepted the requirement to facilitate the increased speed resulting from the technology availability.

# JW-004 Paralon PathKey Domain Series Secure Remote Access

**Sponsor:** Brent Anderson, Paralon Technologies Inc. COMM: (206) 674-4840 FAX: (206) 674-4801, E-mail: banderson@paralon.com



## Description

- Provides access control and real-time encryption between designated databases.
- Provides CTF personnel with low cost, simple to use, rapid and secure remote access to information databases across the range of a CTF command structure.
- Provides ability to structure the flow of and access to information within a limited network.

## Capability Assessment

- The PathKey provided access control and real-time encrypted communications between selected/designated databases.
- The PathKey protected network can be restructured to meet changes in CTF operational participants.
- The product provided access control to selected/designated secure networks.

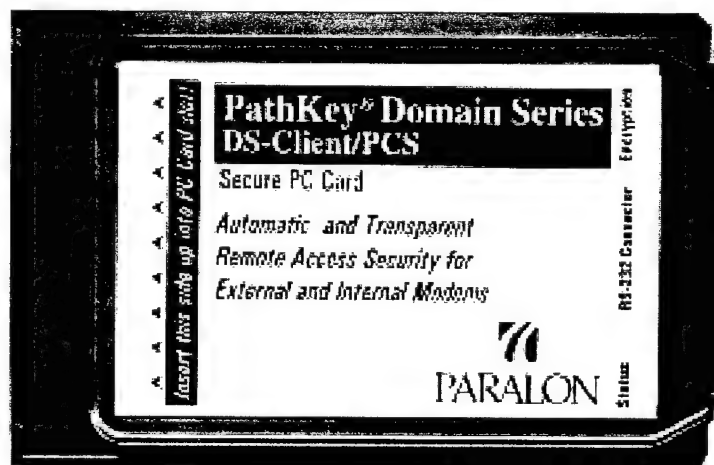
## Objectives Supported

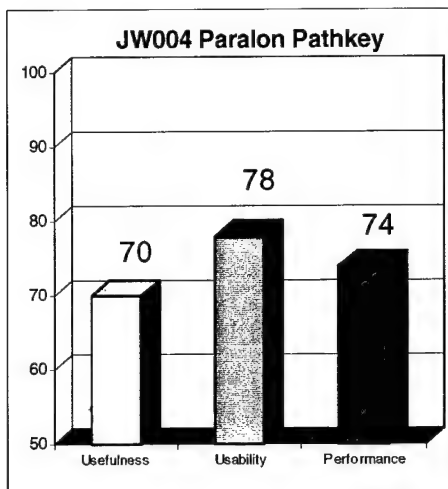
Objective 1 - Not supported because it did not exchange information between multiple levels of security.

Objective 2 - Provided the capability to add/delete/modify access privileges for Paralon PathKey (PPK) users.

Objective 5 - Provided a low cost firewall capability for databases.

Objective 7 - Access denied to non-PPK callers. Unauthorized access was captured and displayed on the systems administrator's terminal.





## Quick Look

- Demo limited to a point to point circuit
- Provided access control and real-time encryption
- Restructured and controlled access to secure network
- Demo utility limited without NSA accreditation for secret level data
- Paralon Pathkey has potential for solving database access control on a CWAN

## Results

**Usefulness – 70%:** Users reported that PPK allowed the passage of encrypted information between point to point users.

**Usability – 78%:** PPK could provide access control capabilities to network users based on classification.

**Performance – 74%:** Messages were sent and received timely and accurately.

## Value Added

PPK provided the capability to protect databases and the size and weight make it an efficient means of security. The system does not transmit the actual security key but sends a negotiable handshake which is only used once and does not require any action by the user to operate. Operators and staff found that PPK had little utility without the ability to handle a minimum of SECRET and/or SECRET RELEASABLE information.

## Conclusions

The system was able to support three of the four objectives as demonstrated, but did not support its primary objective, the exchange of information between multiple levels of security. Operators and staff recognized that the device/system has the potential to safeguard unclassified through SECRET and SECRET RELEASABLE information on the same communications network and on multiple community of interest networks.

## Recommendations

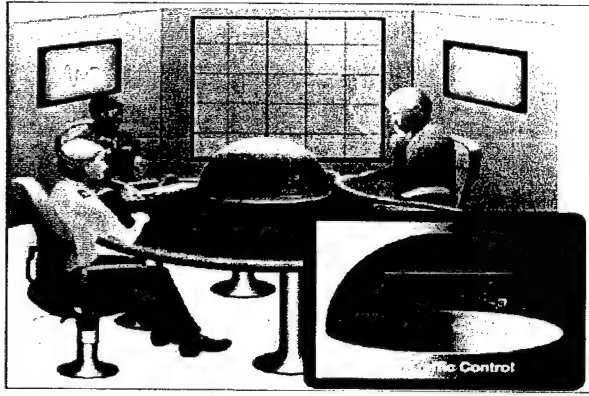
- Expedite NSA approval for use of the appropriate encryption algorithms in PPK.
- Continue development of a system that will:
  - Accommodate unclassified through SECRET and SECRET RELEASABLE information.
  - Provide for multiple users simultaneously.
  - Provide for Service and Allied specific encryption algorithms.
  - Allow system administration from a central site.
  - Develop procedures for the co-existence of PPK and other encryption systems.

## Warfighter Impressions

- System has the potential to safeguard unclassified through Secret/Secret releasable.
- PPK allows the passage of encrypted information between point to point users.
- Messages sent and received were verified to be the same and accurate.
- System very easy to use with minimal training.

**Sponsor:** Jay Martin, NRaD Code D442, (619) 553-4030, martinjl@nosc.mil

**3-D Volumetric Display**



### **Description**

- Demonstrated battlefield awareness.
- Used COP data to generate positional information displayed within volume in a 3-dimensional (3-D) format.
- Demo shifts the 2-dimensional (2-D) paradigm to a 3-dimensional paradigm for situational awareness.

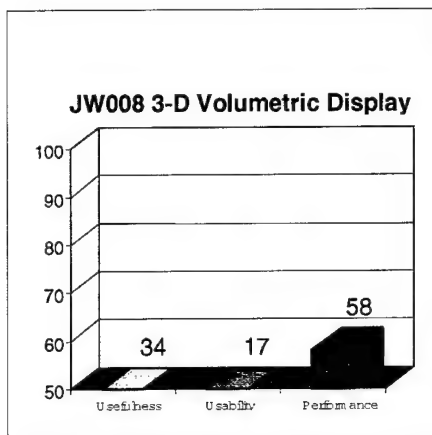
### **Capability Assessment**

- The 3-D representation was set at 40,000 feet with a range of 100 miles. The resulting resolution was 1000 ft in height = .2" and 1 mile in range = .16"
- The 3-D volumetric display has new application software to support the warfighter. The applications demonstrated included; battle group surveillance, fighter-to-fighter target sorting, air control, and mine detection.
- The 16 inch helix display provided a 3D display of 360 degrees, less the support piece, of the battlespace.
- JTIDS units were depicted three dimensionally showing surface, subsurface, and airborne tracks simultaneously.
- The display provided positional information on air, surface, and submarine contacts of hostile, friendly, and neutral powers.

### **Objectives Supported**

Objectives 2 and 3 - The 3-D Volumetric Display provided track data on a 3-D display from the COP in support of objectives 2 and 3. The presentations were unusable and provided no added value to the warfighter.





## Quick Look

- Display exhibited rapid shift motions, flicker, and a faint ghost in presenting a COP picture.
- The distortion above, the size of symbols and use of two colors to show enemy, friendly and neutral tracks and the terrain made the display of little value to the warfighter.

## Results

**Usefulness – 34%:** The warfighter did not have all of the required information to perform the task because the symbology was difficult to interpret, and displays were indistinguishable from other objects.

**Usability – 17%:** The clutter and small size of the display made the system very hard to use for mission accomplishment. The system was not integrated with any other demonstrations. The COP picture had more history data than the 3-D display and the 3-D display could not display the TCP/IP format direct Link 16 Format data feed on the USS John C. Stennis.

**Performance – 58%:** The data feed from Hanscom Air Force Base was not established until Thursday of the second week of assessment. The feed was dependent upon a translation of the COP feed protocol at NRAD to a protocol that the 3-D display could use.

## Value Added

The 3-D Volumetric Display system demonstration was reported by the warfighter to have little utility to the required missions and functions at this time. The display exhibited rapid shift motions, a flicker, and a faint ghost in presenting a COP picture. The distortion above, the size of symbols and use of two colors to show enemy, friendly and neutral tracks and the terrain made the display difficult to view and understand.

## Conclusions

The 3-D Volumetric Display did not show utility or value added to the warfighter and the current approach does not meet the current needs of the warfighter. There is, however, a continued desire on the part of the warfighter to explore the use of 3-D to facilitate battlespace awareness.

## Recommendations

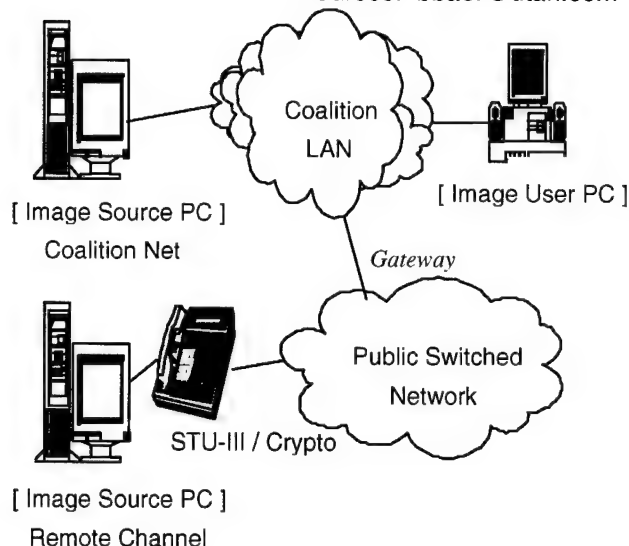
- Continue research in 3-D technology. Must offer full color mapping with relief discrimination and bore-down capability for additional information on icons and tracks.
- Do not consider helix technology at this time for use in a CJTF environment.

## Warfighter Impressions

- Information displayed was not easy to see or understand.
- System was less usable than current operational 2-D displays with 3-D perspectives.
- System had no added value and should not be fielded.



**Sponsor:** William Baer Commercial Telephone: (703) 758-5754 Commercial Fax: (703) 758-5714 E-mail Address: bbaer@titan.com



### Description

- Provides imagery selectable compression, transfer, and analysis tool to increase quality and compression performance.
- Images compressed by a factor of up to 150:1 for color; up to 100:1 for grayscale.
- Timely transmission over low bandwidth comm links retaining critical image details for analysis and intel decision making.

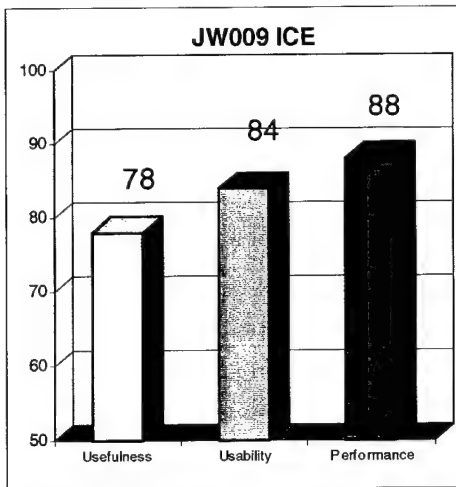
### Capability Assessment

- The ICE demonstration compressed images to user adjusted ratios (up to 150:1 color; 100:1 grayscale). The selectable compression ratios provided a means to balance image quality and file size in order to meet varying operational conditions of restricted transmission bandwidth and transmission time.
- ICE compressed files were easily and accurately transmitted to other Microsoft Windows NT or Windows 95 PC's using existing Internet or email services.
- An ICE configured PC was able to receive ICE compressed files and accurately decompress the files for viewing and editing in the original file format (BMP, TIFF, JPEG, WMF, EPS, CCITT, G3 etc.) with the exception of NITF.

### Objectives Supported

Objective 2 - This demonstration provided a toolkit of advanced compression techniques which enabled the warfighter to select variable compression ratios in consideration of communication path bandwidth, transmission time restrictions and image quality requirements necessary for analysis and decision making. It assisted in the transmission of these images by providing a communications interface (via e-mail systems) for transferring the images and decompression at the receiving site.





## Quick Look

- ICE provided imagery transfer capability not available to the Warfighter.
- Compressed images to user adjusted ratios (up to 160:1 color and up to 100:1 gray scale).
- Reduced bandwidth used for large file transfer.
- Imagery analysts reported that compressed imagery is not significantly degraded.
- ICE is low cost - \$500 per license.
- Compressed 48 different commercial formats.

## Results

**Usefulness – 78%:** The system provided all information necessary to perform the tasks of compressing files for transmission and archival purposes. There are several enhancements that are beneficial, inclusion of a cropping function; porting the software to COE compliant UNIX environment to allow ICE to be incorporated into GCCS and JDISS software suites.

**Usability – 84%:** Operator could tailor the compression ratio to suit the needs of the mission. ICE provided consistent transfer of compressed imagery. Loss of image quality using ICE is not as significant as with other compression techniques.

**Performance – 88%:** ICE provided imagery connectivity to multiple sites during JWID. Files were sent to Australia with minimum degradation. ICE transmitted large data files using less bandwidth and with greater transfer speed.

## Value Added

ICE provided value added to the warfighter by allowing transfer of large imagery data files which were compressed requiring less bandwidth for transmission. The Visual National Imagery Interpretability Rating Scale (NIIRS) was used to judge the clarity of an image. ICE compressed images normally only lost one NIIRS level of clarity as a result of the compression technique. Normally an image in its original state would take twenty to thirty minutes to push through or pull through a 9.6 modem line. The same compressed image could be pushed or pulled through the same 9.6 modem in 1-2 minutes.

## Conclusions

The ICE demonstration provided imagery transfer capability not presently available to the warfighter. ICE actively reduces bandwidth use for imagery transfer. Compressed imagery loss of one NIIRS level is not considered significant to impair its use. The receiving party has to have the ICE software installed to decompress and view the image. The ICE software was practical, easy to learn, and has demonstrated the potential to conserve bandwidth. This system would be extremely helpful to any user with limited or restricted bandwidth.

## Recommendations

- Recommend this demonstration be fielded to the warfighter pending interoperability evaluation.
- Develop capability to read/write NITF format.

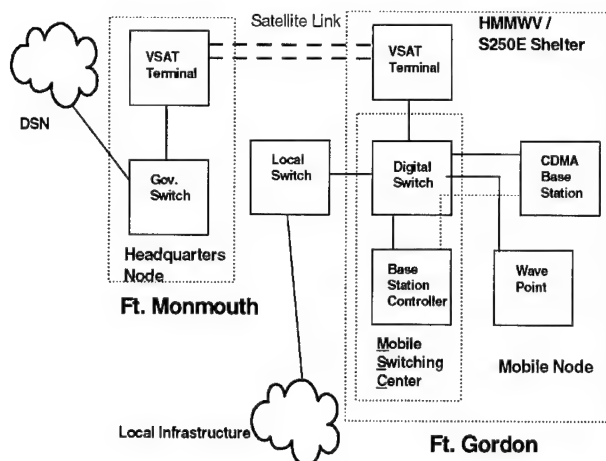
## Warfighter Impressions

- ICE compressed files take less time to transmit with little or no loss in image resolution.
- Easy to use.
- Variable, selectable compression ratio needed for operational conditions.
- Field now.



# **JW-011 *Advance Party Cellular Communications Support With VSAT Backhaul***

**Sponsor:** Mr. Tom Mims, Battle Command Battle Lab, Ft. Gordon, Ga (706)791-3328



## **Description**

- Provided connecting backhaul capability in support of an Advance Party requiring rapidly deployable infrastructure for local and out-of-theater communications.
- Validated the application of commercial CDMA cellular communications with commercial VSAT satellite technology.

## **Capability Assessment**

- Advance Party TacPCS successfully demonstrated the following functions:
  - Provided Mobile-to-Mobile digital cell phone capability for up to twelve simultaneous voice subscribers.
  - Supported a Ku Band VSAT backhaul capability for six voice channels.
  - The TacPCS switching center, composed of Base Station Controller (BSC) and a Mobile Subscriber Equipment (MSE) Switch Multiplex Unit (SMU), could be mounted in standard S-250E shelter on-board a HMMWV and perform successfully.
- Advance Party TacPCS failed to satisfactorily perform the following functions:
  - Provide clear communications using Code Division Multiple Access (CDMA) technology between cell phones; between cell phones and local Digital Nonsecure Vehicular Telephone (DNVT) instruments; and between cell phones and remote landline instruments via Very Small Aperture Terminal (VSAT). While communications could be done, voice clarity was a significant issue.

## **Objectives Supported**

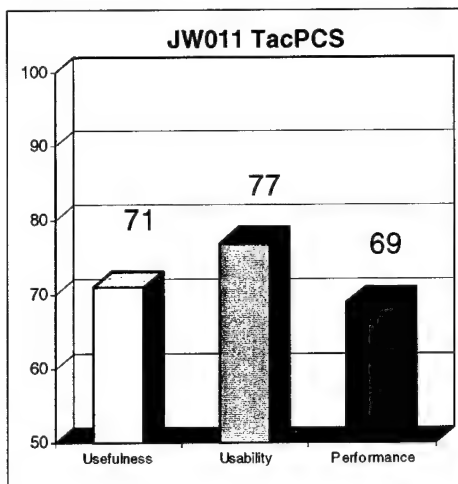
Objective 1 - Unsecured voice communications with other cellular units off the MSE switch was bulk encryption, via government issued trunk encryption devices (TEDs), however only unclassified information could be transmitted over the cellular phones. There were no multi-level security portions demonstrated.

Objective 2 - Only mobile voice wireless with backhaul capability was provided. There were no data or imagery transmissions attempted.

Objective 4 - No sensor-to-sensor or sensor-to-shooter technologies demonstrated.

Objective 5 - Provided assurance of coalition access, use, and integrity of C4ISR systems while preventing unauthorized use of the same. Security and encryption features were not provided.

Objective 6 - Supported by providing mobile cellular voice communications that interfaced both local commercial and military telephone systems as well as remote communication infrastructures.



## Quick Look

- Provided mobile-to-mobile CDMA digital wireless cell phone capability for 12 simultaneous voice subscribers and 6 voice channels for VSAT backhaul.
- Voice quality, limited range/area coverage, secure transmissions, and number of subscribers at one time are critical issues.
- CDMA technology and military use of spectrum is a significant issue, i.e. frequency range.

## Results

**Usefulness – 71%:** Completeness and accuracy of information were based on proximity of cellular unit to antenna and line-of-sight (LOS) sighting with loss of signal results for extended ranges and areas of reception. Interaction was completed with other TacPCS, tactical DNVN over MSE networks, commercial and DSN telephone systems.

**Usability – 77%:** Usability features were not intuitive, particularly in terms of phone book establishment and entries. Completion of attempted dialup and clarity of conversations varied by calls especially in the reachback VSAT mode to remote locations. Security of transmissions needs to be addressed between the cellular unit itself and the bulk encryption entry point of the MSE network.

**Performance – 69%:** Availability of the system was sporadic and was based on the interim authorization to operate within the 1.9GHZ band level provided by the vendor. Significant issues were raised concerning the envisioned future use of the CDMA technology.

## Value Added

TacPCS provided quick set up/tear down capability which could be relied upon while normal command post communications were being established. TacPCS was not designed to take the place of radio access units (RAUs) and Mobile Subscriber Radio Telephone Terminal (MSRT) but to bring the Wireless Tactical Operations Center (TOC) into the present with a rapid set up and tear down functionality.

## Conclusions

Future use of Advanced party TacPCS capabilities will require military procurement of frequency spectrum for CDMA use. The ability to connect laptop or desktop computers and demonstrate data transfer would enhance warfighter acceptance and use.

## Recommendations

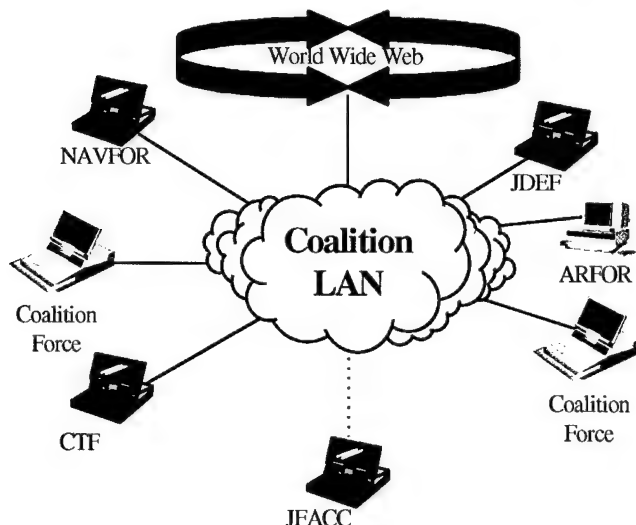
- Resolve security issues and range of deployment measures.
- Improve shortfalls (voice quality, number of users and security).
- Add packet switching capability and 30+ meter antenna.
- Test in an operational/exercise environment after upgrades.
- DoD address CDMA frequency band usage issue for battlefield infrastructure support.

## Warfighter Impressions

- Muffled and choppy transmissions along with “non-secure” beep reminder was disconcerting.
- Wireless concept shows potential for initial TOC setup and operations.
- Lack of security, limited range and LOS requirements impact full utilization.

# JW-012 *Joint Continuous Strike Environment (JCSE)*

**Sponsor:** Mr. Michael W. Casey, Program Manager C4I Integration Support Activity, (703) 883-3355 Fax: (703) 883-1385, E-mail: michael.casey@osd.mil



## Description

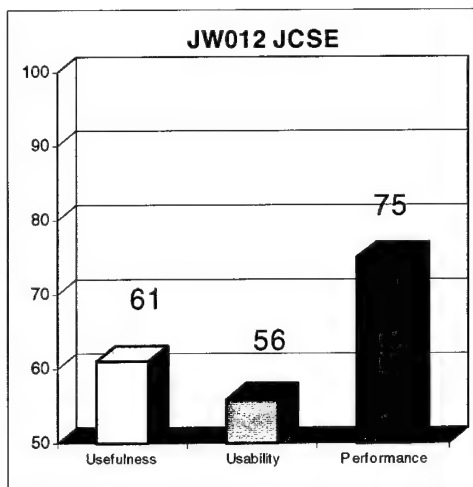
- Demonstrates application of a Joint weapon suite on time-critical targets by selecting service, joint, and combined fire support systems.
  - Automated target prioritization.
  - Continuous weapon availability monitoring.
  - Optimized weapon target pairing.
  - Near real-time airspace deconfliction.
- Consolidates target and weapon information to optimize targeting decisions in the CTF.

## Capability Assessment

- JCSE automatically prioritized targets. It provided a continuously and dynamically updated list of emerging and time-critical targets. JCSE received targets from Naval Weapon Control System (NWCS) and the COP and automatically prioritized them in accordance with the commanders guidance.
- JCSE demonstrated the capability to monitor weapon positions and availability. It automatically received information from NWCS. The operator used a browser to get weapon information from Enhanced AFATDS (EAFATDS). JCSE applied planned information in the ATO to determine other weapon constraints.
- JCSE demonstrated optimized weapon target pairing. JCSE generated and ranked weapon to target options by evaluating assets based on engagement effectiveness (e.g., time, effects, range, etc.) and analyzed attack options with respect to current and projected threat. JCSE generated weapon target pairing options and automatically applied airspace deconfliction. JCSE operators selected desired options and issued the mission to NWCS for execution.
- Near real-time deconfliction was accomplished using ATO and updated ATO information, NWCS information, and tracks on the COP. The COP was used to compare real-time air information to ATO information for deconfliction.

## Objectives Supported

Objective 4 - Demonstrated that information could be shared from service systems and from the Common Operational Picture. JCSE received targeting data from NWCS and the COP. The system demonstrated it could monitor component weapon system availability by receiving ATO data, data from NWCS, and information from the COP. JCSE prioritized targets, matched weapon options to each target, and deconflicted the airspace. The operator used JCSE to forward missions through the CWAN to the components (NAVFOR for JWID). JCSE could not pass information directly to a weapon system. This information was forwarded electronically by the operator to the service systems (e.g. NWCS) and then to the weapon system.



## Quick Look

- Provided staff and operators a capability to combine various sources of information and conduct analysis at the JTF level.
- Forwarded missions through the CWAN to components (NAVEOR and ARFOR).
- Demonstrated optimized weapon target pairing.
- JCSE did not work directly with EAFATDS.

## Results

**Usefulness – 61%:** The system provided the staff and operators a capability to combine various sources of information and conduct analysis at the JTF level. It was reported that more information was needed to complete the mission, for example, when targeting information is shown, the source of the target is also needed. If targets are taken from the component, JCSE needs to identify the priority given the target by the component. Direct connectivity with EAFATDS was not available because the two systems have non-compatible formats. If the JMCIS portion of EAFATDS had been permitted to operate in demonstration JW043, weapon position and availability information could have been transferred.

**Usability – 56%:** The system was easy to use and its automation made it easier to complete tasks. JCSE allowed the operators to complete their tasks in a timely manner. The on line help information is still being developed and requires more user input.

**Performance – 75%:** JCSE was available when needed. There were some problems with CWAN availability.

## Value Added

JCSE provided improved capabilities for the operators and staff to complete their tasks, but most would not field the system now. The potential for the system was noted, but most reported that the system needed more information on which to base decisions and that the current algorithms were too simplistic. Operators and staff also stated that more flexibility was needed for commanders to input priorities on a continuing basis and for staff officer judgment input on the validity of information.

## Conclusions

Doctrinal issues, such as the role that humans must play in the targeting process, the scope of targeting at a central site, and what processes can be automated, needs to be defined. The required information (e.g. weapon capability, ground force location, boundaries, etc.), from various National, Allied and Service systems needs to be determined to support objective/mission decisions.

## Recommendations

- Define and analyze the doctrinal usage of the system.
- Continue development as a potential target/weapon manager at the Coalition and Joint Level.

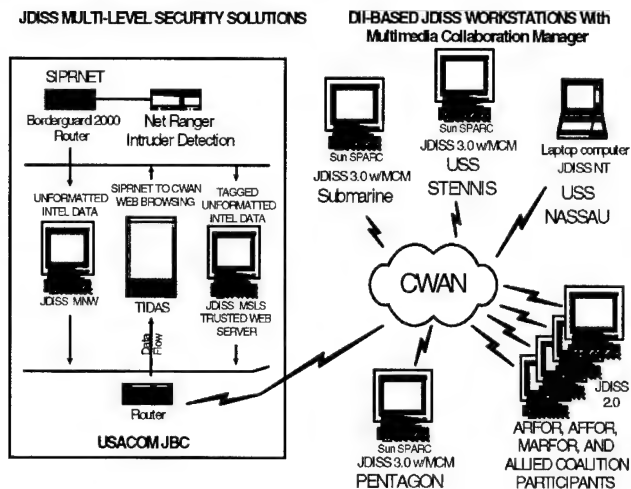
## Warfighter Impressions

- Great potential.
- Would not take to the field now.
- Needs to provide more information to complete mission.
- Easy to use.
- Warfighter not comfortable with power and responsibility JCSE provided.

# JW-015 *DII-Based Joint Deployable Intelligence Support System (JDISS)*

**Sponsor:** CDR Vivian Turnbull, USN, ONI-71 (301) 669-4713, 4251 Suitland Rd, Washington, DC 20395

## Description



- JDISS 3.0 (DII COE 3.0) for UNIX (Solaris) & NT systems provided interoperability & collaboration with GCCS.
- JDISS MNW allows operator to push non-formatted intelligence products from SIPRNET and LOCE to CWAN.
- TIDAS allowed SIPRNET and LOCE users to Web browse across LAN interface to CWAN servers.
- MSLS Webmaster provided Coalition-releasable US intelligence access from CWAN browsers.
- NetRanger COTS monitored activity as proactive real-time network intrusion detector.

## Capability Assessment

- DII-based JDISS 3.0 UNIX and NT workstations provided a family of interoperable tools for basic intelligence and imagery analysis at the JBC, JDEF, Stennis, Atlanta, and Nassau.
- JDISS Multi-Level Security (MLS), Multi-Network Workstation (MNW) and Multi-Security Level Server (MSLS) systems provided a means for an operator to disseminate data and products to/from Coalition Wide Area Network (CWAN), SIPRNET, and Linked Operations-Intel Center Europe (LOCE) networks at the JBC.
- The Trusted Intelink Dissemination Access Servers (TIDAS) provided ability for designated hosts on the SIPRNET and LOCE network to "browse down" to designated web sites on the CWAN.
- The JDISS Multimedia Collaboration Manager (MCM) segment provided plug-in collaborative planning and VTC enhancement for DII-based UNIX systems e.g. JDISS 3.0 (at the JBC, JDEF, Stennis, and Atlanta).
- NetRanger system was able to detect CWAN intrusion attempts on the JDISS MLS systems at the JBC.

## Objectives Supported

Objective 1 - MSLS, MNW, and TIDAS demonstrated information exchange between SIPRNET, LOCE and the CWAN.

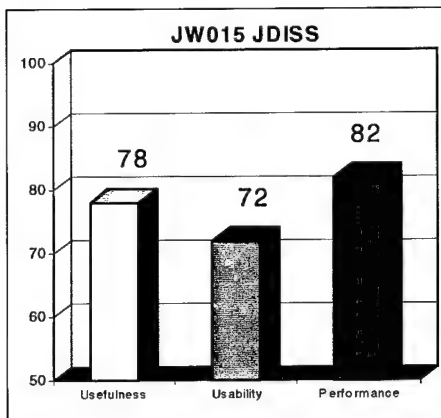
Objective 5 - NetRanger was able to detect intrusions into the JDISS segment of the CWAN and audit activity between the JDISS MLS system and the CWAN.

Objective 6 - Standard JDISS COTS and GOTS tools used in an integrated fashion to provide intelligence support.

Objective 7 - Full JDISS 3.0 (NT and Solaris) DII Compliance was shown to improve JDISS utility and interoperability to the Coalition Joint Task Force (CJTF).

Objective 9 - JDISS 3.0 capabilities were demonstrated on Windows NT 4.0 workstations.





### Quick Look

- COTS/GOTS tools promoted interoperability between JDISS, MNW, NT, TIDAS, and other demon.
- JDISS 3.0 DII compliance and NT and Solms gave the system a plug and play capability.
- FORTEZZA provided level of access control not currently available.
- JDISS on an NT-based personal computer sponsored training and increased use of the system.
- MSLS systems offered a solution for disseminating intelligence products in a Coalition environment.

## Results

**Usefulness – 78%:** Warfighter found system useful. Demonstration provided the ability to pass information from one security level network to another while providing a “man-in-the-loop” control point to oversee the movement of the information between the SIPRNET, LOCE, and CWAN networks.

**Usability – 72%:** The Multi-Network Workstation easily transferred complete intelligence products when needed. Applications were standard across the JDISS systems. Lack of standards for mail applications, browsers, and imagery file formats, sometimes caused problems in transferring information across networks and to other demonstrations.

**Performance – 82%:** System was considered reliable. Setup continued past set-up week due to software problems and limited technical support to the afloat units. LOCE experienced some software problems. MCM capabilities were slow to be established due to communication link problems between the afloat units.

## Value Added

The primary value-added of MSLS, MNW, and TIDAS was the ability to pass information from one security level network to another while providing a “man-in-the-loop” control point to oversee the movement of the information between the SIPRNET, LOCE, and CWAN networks. It allowed the operator to quickly and efficiently move intelligence products between these networks.

## Conclusions

MNW, MSLS, and TIDAS offered a solution to the problem of disseminating tailored intelligence products in a Coalition environment. They improved the timeliness and efficiency of sanitizing/passing information from one Coalition network to another while providing a secure “man-in-the-loop” gateway/control point to verify classification and need-to-know. NetRanger gave the operator a level of control over CWAN access to the JDISS systems, which provided a new level of security for the systems by fulfilling an emerging need to protect against both internal and external intrusion attempts. JDISS 3.0 DII compliance gives the system a plug and play capability. FORTEZZA provides a level of access control not currently available.

## Recommendations

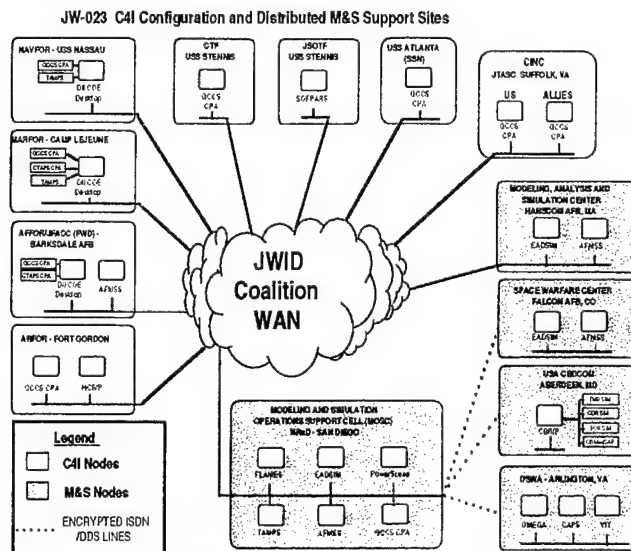
- Field MNW, MSLS, and TIDAS, while continuing to enhance the systems for future releases, and integrate these MSLS systems into JDISS.
- Based on improved capability/usefulness, field JDISS 3.0 to the warfighter and continue efforts to make JDISS cross-platform accessible by porting MCM to the NT version.
- Standardize office automation applications and email clients that are interoperable across UNIX and NT.

## Warfighter Impressions

- A critical requirement for coalition operations.
- Significant improvement to efficient, timely mission accomplishment.
- Improved intelligence database.
- Send to the warfighter now.

# JW-023 *Modeling and Simulation Support to C4I in the DII COE Warfighting Environment (COMPASS)*

**Sponsor:** CDR Donald McSwan (NRaD) Code 808, Commercial (619) 553-9711, DSN 553-9711, mduck@nosc.mil



## Description

- Provided modeling and simulation services to C4I systems by enhancing interoperability between systems across all coalition boundaries.
- Provided distributed collaborative planning services that support development, testing, rehearsal, and after the fact review of events.
- Supports the warfighter conduct of operational planning with and between DII COE compliant and non-compliant systems.

## Capability Assessment

- COMPASS provided distributed collaborative "planning tools" and Modeling and Simulation capabilities not otherwise available to DII COE and legacy systems. The services provided include: distributed collaborative plan development preview assessment and revision.
- COMPASS services supported the following activities: Draft and final courses of action, campaign plans, mission plans, plan assessments, final plans, and revisions of plans to be sent to operational components and elements via traditional means of dissemination.

## Objectives Supported

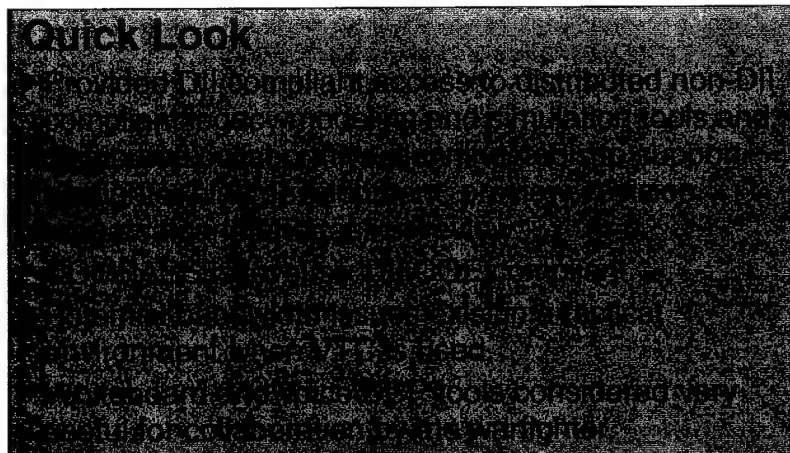
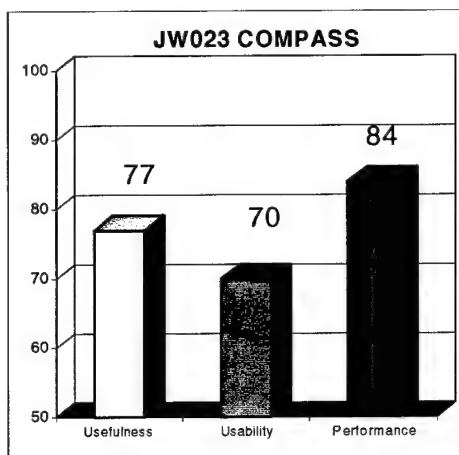
Objective 2 - Provided a common method of delivering warfighting plans, imagery, other intelligence information, and plan analysis with assessment to all echelons through the integrated GCCS platform.

Objective 6 - Provided a wide range of automated distributed collaborative planning tools to DII COE hosted systems and interoperability to non-DII COE distributed legacy modeling and simulation tools. The coalition warfighters were able to build coalition campaign mission plans, test them through modeling and simulation, revise them and provide a common, proven mission plan to be executed by the Coalition Joint Task Force.

Objective 7 - Enhanced utility of the DII enabling warfighters to conduct operational planning with non-DII modeling and simulation legacy systems, to access and collaboratively share plans, and to share products and information to/from DII-Compliant C4I systems.







## **Results**

**Usefulness – 77%:** COMPASS presented information provided by other systems and allowed mission planners to review, collaborate and plan, simulate and re-evaluate those plans based upon M&S results. It allowed the exchange of information to and from DII and non-DII systems. With the number and diversity of sites and users, COMPASS demonstrated its ability to interact and interchange information through the services provided by distributed collaborative planning tools. COMPASS PHASE II is a sophisticated set of tools with a primary purpose of providing modeling and simulation services supported by the interaction and exchange of information provided by distributed collaborative planning tools.

**Usability – 70%:** Some operators were uncomfortable with a Unix based system and thought that a Windows environment would be easier to use. Many human factors issues were discussed, such as the need for a hour glass or clock to indicate that the machine is processing.

**Performance – 84%:** COMPASS was available for most sites after initial set up issues were resolved. One site had a two day outage caused by a bad disk.

## **Value Added**

COMPASS provided significant value to the warfighter by accessing legacy modeling and simulation systems and providing DCP to support planning, assessment, review, revision, and rehearsal of plans. COMPASS allows plans to be tested prior to execution.

## **Conclusions**

COMPASS has great potential for the warfighter-planner. Responsiveness and bandwidth usage issues in tactical environments need more assessment, but should not delay implementation at higher levels. All collaborative planning tools should be assessed together before determining the role of COMPASS in operations.

## **Recommendations**

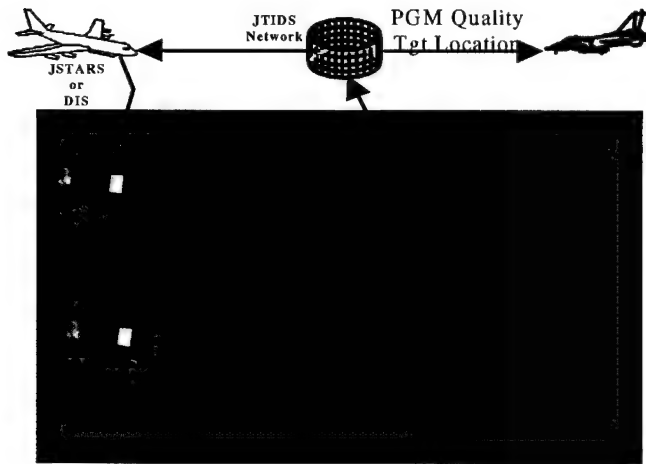
- Field system to increase warfighter ability to plan and rehearse.
- Investigate COMPASS responsiveness and bandwidth issue in tactical environments.
- Integrate address book into COMPASS.
- Investigate moving COMPASS to a PC.
- Assess all DCP tools and the part each should play in an integrated C4ISR system.

## **Warfighter Impressions**

- Warfighters liked COMPASS features.
- COMPASS saves time (measurable in days) for mission planners.
- COMPASS allows plan testing and modification prior to execution.
- COMPASS has outstanding white-board and audio sessions.
- Some warfighters see the system as not responsive enough to make real-time decisions in support of execution.
- Needs to be more user friendly.

# JW-028 JSTARS Imagery Geolocational Improvement (JIGI)/Time Critical Targeting Aid (TCTA)

**Sponsor:** Capt Ashabranner, Capt Taraska, Air Force Electronic Systems Center Comm (617) 377-8453



## Description

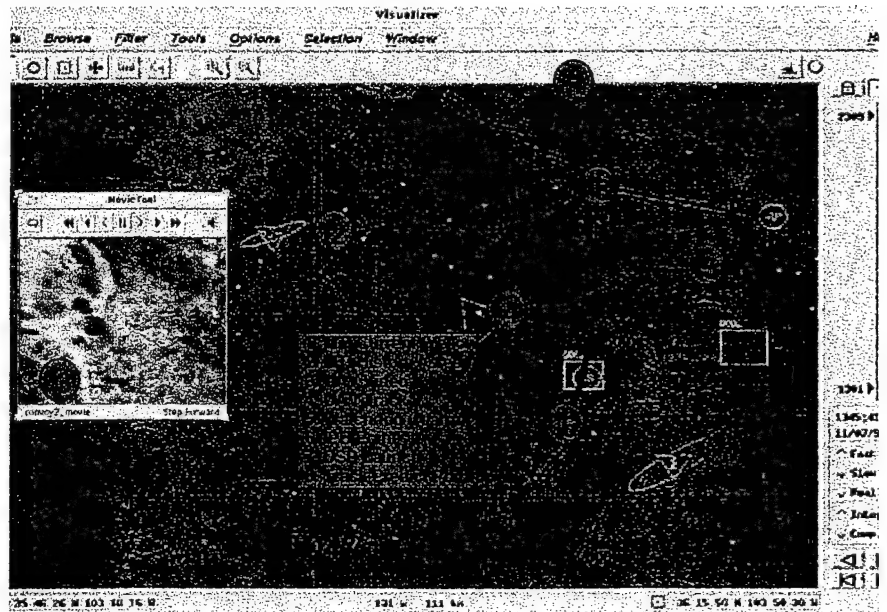
- Enhances the value of sensor data at Theater Missile Defense (TMD) Command and Control (C2) nodes, such as the AOC, and in application of stand-off weapons.

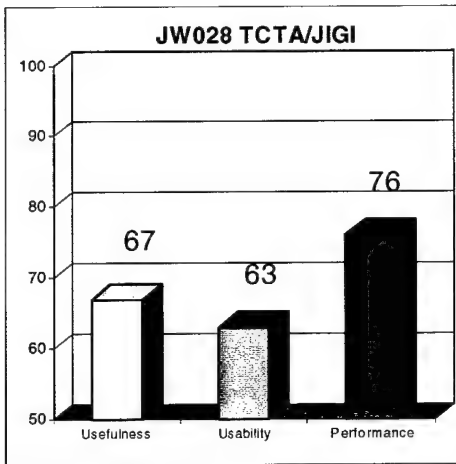
## Capability Assessment

- TCTA demonstration software provided near real-time (NRT) Intelligence and targeting operation tools for locating time critical targets.
- The JSTARS Imagery Geolocational Improvement (JIGI) demonstration software, a modified version of the Multi-Image Exploitation Tool (MET), produced targeting-quality geolocational information by registering imagery collected by JSTARS' on-board sensor with archived national imagery.
- TCTA/JIGI products and derived target locations were provided to the COP.

## Objectives Supported

Objective 4 - Successfully demonstrated to the TCTA operators the ability to track and target hostile Transporter Erector Launcher (TEL) target's (e.g. SCUD's) by displaying accurate tracking information generated by the JSTARS Synthetic Aperture Radar (SAR). This information was displayed through a Moving Target Indicator (MTI) format, which in combination with signal intelligence (SIGINT) overlays and JIGI enhanced locational data, provided accurate and timely tactical information critical in TMD operations.





## Quick Look

- TCTA/JIGI provided AOC personnel a new capability to track and target TMD targets in real-time using JSTARS input.
- TCTA/JIGI provided improved positional accuracy for use in targeting TMD tracks.
- TCTA/JIGI at Barksdale was unable to send tracks to COP, however, Hanscom was successful.
- Software was user friendly.

## Results

**Usefulness – 67%:** The inability to label and prioritize imagery targets slowed the process for time-critical targets. The system integrated well with JIGI, however, operators indicated that the system should interoperate with other information systems to meet all requirements.

**Usability – 63%:** The ability to access intelligence databases is needed to increase information available to the operator.

**Performance – 76%:** The demonstration was frequently down due to SIPRNET connectivity problems. Operators were unable to evaluate the full potential until near the end of the exercise. No launch reports were available and the simulation did not provide the required data. Operators indicated that the system was reliable once connectivity was established and data began to flow.

## Value Added

TCTA/JIGI provided AOC personnel an added capability to track and target time-critical TEL targets that had not previously been available.

## Conclusions

The overall assessment from the operators is TCTA was an invaluable asset to have for TMD operations, filling a critical C4I requirement. The TCTA/JIGI system will allow AOC personnel to effectively track and target TELs using JSTARS SAR and enhanced locational data, accurate enough for targeting. The availability of historical data within the system allows for the analysis of hostile TEL operations and serves as a planning tool. User friendly enhancements and additional interoperability with other information systems would increase its value. The exercise itself did not provide the means to fully evaluate the capabilities of TCTA due to simulation limitations and set-up week delays.

## Recommendations

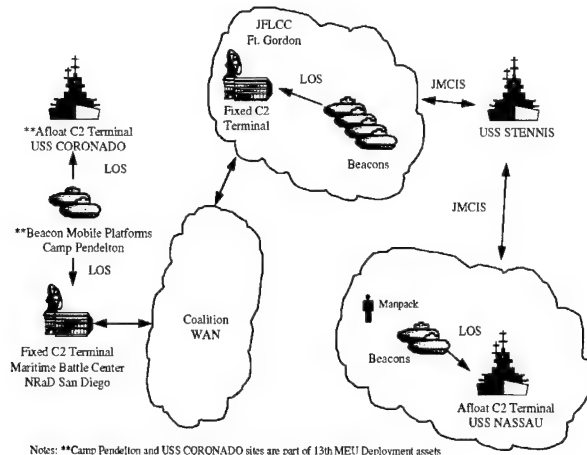
- Field TCTA/JIGI as a TMD tracking and targeting tool.
- Make MTI symbology larger and easier to identify.
- Package JIGI with a graphical user interface.
- Provide interface coordinate display corresponding to cursor position.
- Provide a labeling capability for the imagery to allow easier identification.
- Provide a means to click-and-drag over an area and to query its imagery.
- Further develop TCTA/JIGI software for easier use.

## Warfighter Impressions

- Functions and connections to systems (GCCS, etc) need to be added.
- Lack of realistic info from JSTARS along with inadequate simulation data impacted true assessment.
- Too many operator functions and constant eyes-on-screen became labor intensive.

# ***JW-032 Situational Awareness Beacon with Reply (SABER)***

**Sponsor:** LTC John Authur, USACOM J332M2, (757) 327-7857, DSN 836-7857,  
arthurj@doim6.monmouth.army.mil



## **Description**

- Provides real-time location info derived from GPS positional info and platform data that is disseminated to the theater tactical assets and global C2 nodes via UHF LOS and UHF SATCOM reporting links.
- Supports Combat Identification (CID) by combining friendly force Situational Awareness (SA) information with direct identification of friendly combat assets.

## **Capability Assessment**

- SABER beacons, on mobile units, provided the mobile warfighter with real-time location information derived from the Global Positioning System (GPS).
- SABER beacons, on mobile units, provided real-time position location information (PLI) to the fixed C2 terminals (or C2 JMCIS software segments) via UHF LOS and/or UHF SATCOM.
- SABER beacons provided friendly ID (FID) to prevent fratricide in a friendly sector.

## **Objectives Supported**

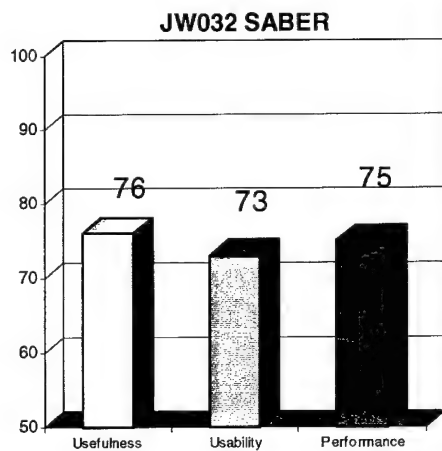
Objective 2 - Provided real-time PLI of friendly force assets directly into the COP through a segment of the JMCIS system.

Objective 3 - Provided automatic real-time GPS position data from ground vehicles, dismounted Special Operations Forces (SOF) and LCACs, ship tracks, and HELO tracks, through the USS Coronado's CWAN connection. All tracks were fused into the COP through JMCIS and provided to Coalition forces over the CWAN.

Objective 4 - SABER was specifically designed for the SA and CID function. SABER participants can see all other SABER units around their position, and the SABER friend identification (FID) network allows individual SABER beacons to query a weapons impact point to check for friendly forces before firing.

Objective 7 - Exchanged data directly with the JW085 COP demonstration as well as JMCIS and USMC versions. SABER's direct feed to JMCIS/GCCS will make SABER interoperable with all Services and Allied forces.





## Quick Look

- SABER provided real-time SA and CID to maneuvering combat assets and real-time friendly force disposition to the CJTF.
- Interoperable with JMCIS/GCCS.
- Feeds from SABER to COP provides significant value added in preventing fratricide.
- Shared blue-force Position Location Information (PLI) with all Services and Allies.
- SABER enhanced the ability to navigate and rendezvous with other tactical units.

## Results

**Usefulness – 76%:** SABER provided enhanced CID information to the warfighter, and eliminated the requirement for manual plotting of old unit information. SABER enhanced the ability to navigate and rendezvous with other tactical units for logistic support.

**Usability –73%:** SABER SA and FID displays are easy to understand and use. The installation and reconfiguration time (LOS to SATCOM) are minimal.

**Performance - 75%:** The SABER beacons and antennas are rugged and easily installed and uninstalled. The “one size fits all” beacon can be moved from manpacks to vehicles as required.

## Value Added

SABER enhances the Tactical Commander’s ability to accomplish his mission by providing two critical elements for maneuvering combat units: (1) friend identification from a direct query of the SABER network before firing into an area and (2) real-time automatic updated blue force SA. Provided the CJTF with real-time friendly force disposition.

## Conclusions

SABER provided real-time SA and CID to maneuvering combat assets and demonstrated a significant C2 tool capability from the tactical shooting asset up through various levels of Command. Its interoperability with JMCIS/GCCS facilitated sharing of real-time blue force PLI with all Services and our Allies via SIPRNet, NIPRNet, and the CWAN, and provided the CINC/CJTF with real-time friendly force disposition. In its current prototype form, SABER can be fielded as a quick-fix system. SABER needs some enhancements to reach full potential. Upgrading its encryption capability to a NSA level one, would allow threat tracks and intelligence information at the C2 terminal (fed from the COP) to be sent directly to a tactical vehicle’s SABER display. The SABER beacons and antennas are rugged, but they need to field a more rugged CDT display for the tactical vehicle. The SABER concept/capability is mature enough to be embedded in existing/future radios/platforms that have a GPS and/or UHF LOS/SATCOM capability.

## Recommendations

- Field SABER as a near term inexpensive blue force SA and CID device, but ensure that a more rugged tactical display is provided to the tactical asset.
- Ensure that the production version of SABER has a NSA approved Crypto capability.
- Investigate integrating the SABER capability into existing/future multi Service digital radios.
- Build a smaller manpack version of SABER for the dismounted application.

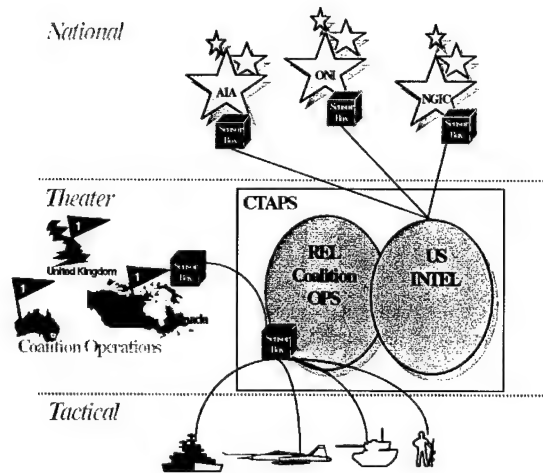
## Warfighter Impressions

- Need system now.
- The system enables troops to better identify one another so as to avoid fratricide.
- Tracking and prevention of fratricide capabilities work great.



# ***JW-036 Sensor Box - Intelligence Support To The Warfighter***

**Sponsor:** Capt Robert Caley, USAF, HQ Air Intelligence Agency DOML, (210) 977-3719, recaley@mail.aia.af.mil



## **Description**

- Provides coalition forces direct access to coalition releasable data spaces of the Air Operations Center (AOC).
- Allows the coalition warfighter to use a single query to retrieve releasable information Intel, imagery, operations databases, and open source info required to support development of target mission folders.
- Data presented to user in an integrated and concise manner using an Intelink browser.

## **Capability Assessment**

- Sensor Box permitted Joint and Coalition forces to access intelligence and operational information supporting execution of Air Tasking Orders (ATOs).
- Sensor Box allowed use of existing tactical platforms/workstations such as GCCS, CIS, CTAPS, JDISS to be used by authorized users without additional software procurement.

## **Objectives Supported**

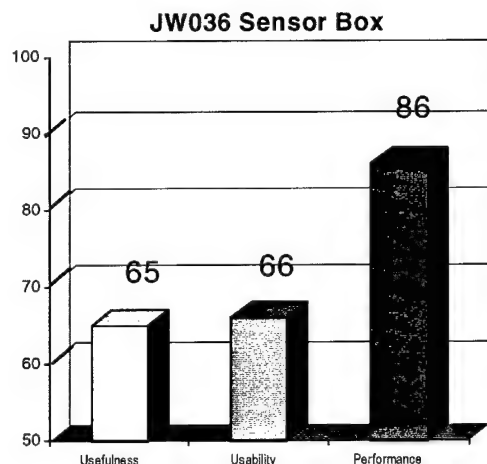
Objective 1 - Did not exchange information between multiple levels of security. Sensor Box provided an interface to the trusted coalition scenario database but did not provide a MLS capability.

Objective 2 - Provided a single integrated front-end browser to multiple operational databases on the CTAPS and other systems. This used less bandwidth than conventional client-server implementations. Sensor Box permitted the end user to enter a single structured query and obtain pertinent data from the various system databases.

Objective 5 - Did not address issues of information operations/information warfare such as C2 protect. The Sensor Box demonstration provided access to 'authorized' users but did not provide indications and warnings of intrusion beyond the system login and access established for the CWAN.

Objective 6- Built around COTS products (Netscape, Delphin Envoy, Enter Works) and supports split-base operations by providing a 'thin-client' interface to operational data.





## Quick Look

- The UK was able to access Sensor Box through Netscape and receive coalition data.
- Sensor Box was shown to be accessible via a GCCS platform.
- Interfaced with JW068 for ATO generation.

## Results

**Usefulness – 65%:** Gave the warfighter the information required to perform all required functions in a timely manner. The system allowed interaction between all designated systems, and information retrieved was verified to be accurate.

**Usability – 66%:** The system was very easy to use. Information could be accessed and viewed quickly from multiple data sources that would normally require complex queries.

**Performance – 86%:** Although the availability was generally good, there were a number of problems with this system, which required system administrator intervention.

## Value Added

Sensor Box provided the warfighter the ability to accomplish his mission(s) in a more effective manner. It allowed the user, through a single query, to view data from multiple sources without the user requiring knowledge of the distant-end data schema and structures.

## Conclusions

Sensor Box proved to be user friendly and displayed a variety of operational and intelligence data in a readily comprehensible format. It provided Joint and Coalition warfighters a single web browser interface with intelligence and operational information. The single query design allowed users to access information with minimal training. The warfighter and the decision-maker were able to view available information needed with a single query. Sensor Box requires access to additional databases and refinement, but would be helpful for the warfighter, if fielded in its current configuration.

## Recommendations

- Add additional databases as well as targeting and analysis tools.
- Demonstrate database access of real-time data from multiple sites and the ability to integrate the query response.
- Add data source tags to query responses.
- Develop a Concept of Operations.

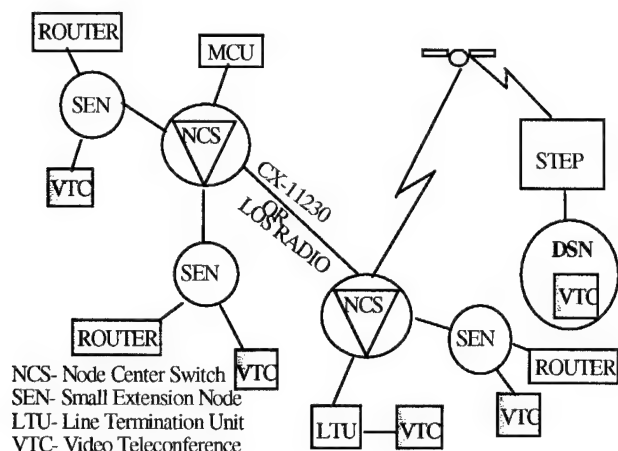
## Warfighter Impressions

- Useable system but requires further development.
- Has potential.
- Need to tag data as to source for improved confidence factor.
- Demonstrate using real database data vice demo data.
- Develop a Concept of Operations.



# JW-039 *Battlefield VTC/Collaborative Planning and Data (BVTC)*

**Sponsor:** Ed Marsh, GTE Gov't Systems, 508-880-4823, Ed.Marsh@gsc.gte.com



## Description

- Provides a tactical VTC capability that does not require ATM.
- Uses existing systems to provide multicast VTC between Brigade and Division TOCs and other elements.
- Uses a new HSMUX/DEMUX circuit card and modified switch software that allows the initiating VTC to "automatically dial-up" the needed connections across MSE and TRI-TAC systems.

## Capability Assessment

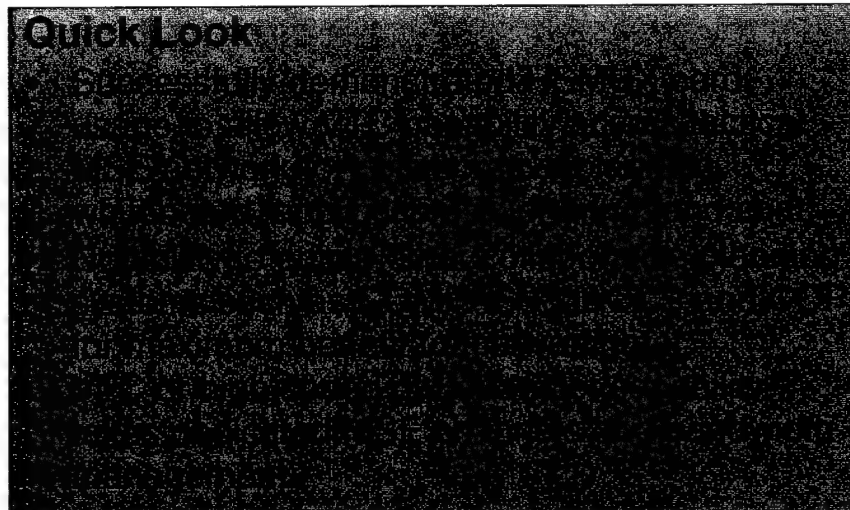
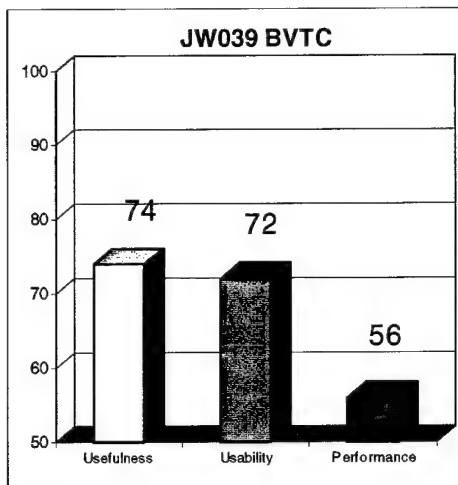
- The new Small Extension Node (SEN) High Speed Multiplexer (HSMUX)/DEMUX provided video teleconference (VTC) capabilities between terminals.
- The VTC Software installed at the National Command System (NCS) allowed the initiating VTC terminal to establish a video teleconference automatically without operator intervention. Upon completion of the VTC, the software released assigned communication assets.

## Objectives Supported

Objective 2 - Modified existing MSE equipment (replacement of the High Speed Multiplex card) and capitalized on techniques used in the commercial telecommunications industry to allow the warfighter to conduct VTC/collaborative planning over tactical circuits.

Objective 6 - Used COTS and GOTS equipment to provide consistent data (as well as VTC and collaborative planning tools) exchange between in-garrison and deployed elements of the CTF.





## **Results**

**Usefulness – 74%:** Using the HSMUX card, there is a value added by projecting a collaborative planning and VTC capability to deployed field locations. Time, safety, and logistical transportation requirements are enhanced with use of this capability.

**Usability – 72%:** System is easy to use and requires the operator have a basic Windows background. Replacement of the HSMUX card is simple. It functions like the original card but with a higher throughput.

**Performance – 56%:** Battlefield VTC (BVTC) is the first time COTS VTC has been available over a tactical Mobile Subscriber Equipment (MSE) circuit and proved to be reliable. A fully operational MSE system may have difficulty managing the dedicated bandwidth requirements for the VTC capability due to the requirement for 16 dedicated MSE channels.

## **Value Added**

The added value of BVTC is the use of commercial VTC equipment, which is currently in place on many military desk top computers. This commercial equipment allows collaborative planning over the tactical MSE system by replacing the current MUX/DEMUX card with the HSMUX/DEMUX.

## **Conclusions**

The only additional equipment required, above the desk top computer and VTC equipment, was an interchangeable HSMUX card and a CISCO router for high volume data distribution. The HSMUX card offered distinct advantages by bringing VTC technology to the field environment over tactical circuits. Three limitations surfaced during the demonstration: 1) 16 dedicated MSE channels are required to operate the VTC or high speed data; 2) modifying the database for SEN units and internodal links was planning intensive; and 3) active MSE network management of the bandwidth is required. Emerging data compression techniques and active management of the 256Kbps pipe could assist in solving these kinds of bandwidth shortfalls.

## **Recommendations**

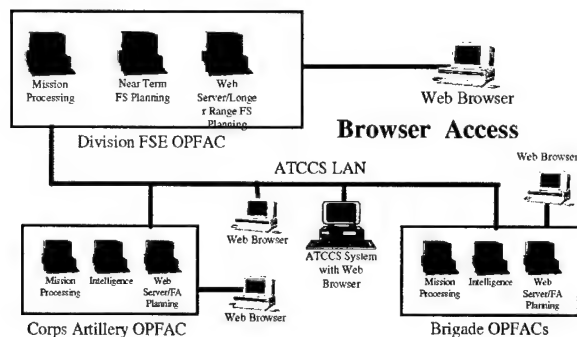
- Assess in a large operational/exercise scenario with multiple tactical users.
- Examine extension of HSMUX and VTC capability over to COMPASS, JACCS, and COP with an extension to CTAPS, JMCIS, and AGCCS.
- Upgrade collaborative tools w/pull down menus and incorporate military symbols and graphics.
- Port Battlefield VTC technology to other Service's tactical switches.

## **Warfighter Impressions**

- User friendly; a system of the future with excellent image resolution.
- Faster data processing and with capability for VTC via tactical circuits.
- Field the HSMUX cards in every MSE assemblage for warfighter use as required.

# JW-043 *Joint Attack Command and Control System (JACCS)*

**Sponsor:** LTC William Drummond, Product Manager, AFATDS, Ft. Monmouth, NJ (908) 427-3328



## Description

- JACCS is a low cost web technology enhancement of AFATDS that extends fire support situational awareness to Web browsers on user provided platforms.
  - Achieved direct AFATDS interoperability with UK BATES fire support system.
- Whiteboard and video conferencing extend fire support planning, coordination, and execution to joint and coalition forces without need for AFATDS equipment.

## Capability Assessment

- JACCS provided fire support data retrieval and input via commercial web browsers with whiteboard capabilities and VTC.
- The JACCS allowed non-JACCS systems to interoperate with Advanced Field Artillery Tactical Data System (AFATDS) 97 baseline software databases.
- JACCS featured vector maps to depict terrain detail. The maps provided a zoom-in/zoom-out capability depicting a common terrain picture with overlay symbology.

## Objectives Supported

Objective 1 - Provided near real-time data exchange incorporating Web Browser technology to facilitate interoperability between US and Allied/Coalition forces.

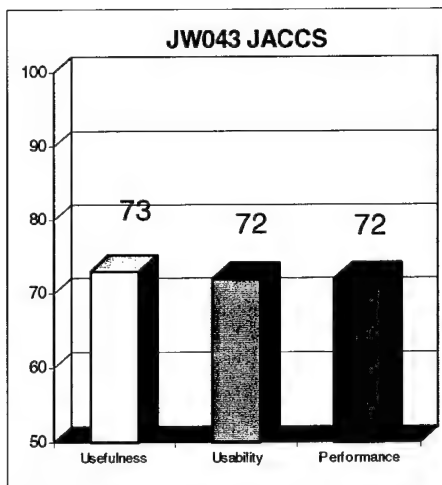
Objective 2 - Used TCP/IP protocols to allow data delivery over-the-horizon from shore based JACCS to ship borne JACCS.

Objective 3 - Provided Vector Maps produced by the National Imaging and Mapping Agency (NIMA) to depict terrain detail.

Objective 4 - Provided AFATDS 97 baseline capabilities with linkages from sensors to delivery platforms for joint and coalition system and demonstrated strike threads from identification of high payoff targets, to target pairing, into the fire process coordination and assignment of fire units to engage the targets.

Objective 6 - Featured COTS integration through the use of Netscape's Enterprise Web Server. Additionally, the interface to the United Kingdom (UK) Battlefield Artillery Target Engagement System (BATES) and connectivity to JACCS locations for both ship and shore units was facilitated by use of the web browser.





## Quick Look

JACCS is a web-based extension of AFATDS that enables collaborative fire support planning, coordination, and execution across multiple command levels. JACCS was used by the 1st Airborne Division, 1st Air Cavalry Division, and 1st Air Cavalry Division (Airborne) during the 1995-1996 operations in the Balkans. JACCS was used by the 1st Airborne Division, 1st Air Cavalry Division, and 1st Air Cavalry Division (Airborne) during the 1995-1996 operations in the Balkans. JACCS was used by the 1st Airborne Division, 1st Air Cavalry Division, and 1st Air Cavalry Division (Airborne) during the 1995-1996 operations in the Balkans.

## Results

**Usefulness – 73%:** The ability to collaboratively draw on graphics and overlays was used to plan effectively. JACCS accessed and conducted planning with other command levels, but better scenario scripting at other demos would have facilitated JACCS utilization.

**Usability – 72%:** JACCS was easy to learn and use. Collaboration and exchange of information was also easy.

**Performance – 72%:** The JACCS allowed real-time fire support C2 from anywhere on the CWAN to any of five locations with AFATDS Web servers. Lower end laptops at several sites experienced sporadic failure of the COTS Web browser software. This was attributed to insufficient memory ( $\leq 16$  MB RAM) and slow 80486 processors. Performance was measurably higher with COTS Web browsers hosted on more capable systems. The AFATDS interface to the U.K. fire support system, BATES, was highly effective.

## Value Added

JACCS allowed inexpensive existing COTS software (web browser technology) to communicate with the already fielded AFATDS. Whiteboard and chat features allowed smaller deployed units or allies, who would not normally have a full AFATDS system, to collaborate and plan fire support missions.

## Conclusions

JACCS provides an inexpensive way to extend the AFATDS capability to other units/Services/Allies that do not have the AFATDS system to access the database. Video teleconferencing was not demonstrated due to technical incompatibilities between the video hardware and the CWAN. Whiteboard techniques and chat feature allowed real-time distributed manipulation of screen elements from multiple and dispersed operational facilities (OPFACs) increasing the effectiveness of collaboration in a distributed environment. Real-time information exchange between multiple levels of security at the Coalition Task Force/component level is required to fully utilize the AFATDS capability.

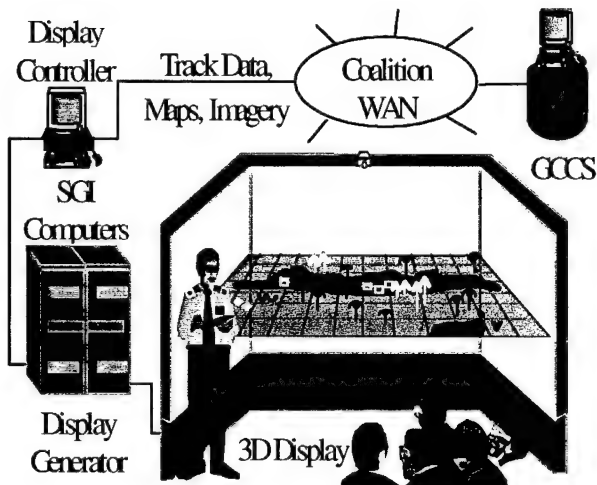
## Recommendations

- Incorporate JACCS with AFATDS.
- Capitalize on AFATDS-U.K. BATES interoperability by expanding functionality to other allies.
- Expand joint functionality requirement and cross training and formalize AFATDS interfaces with Service systems such as JMCIS, TCS, and TBMCS.
- For most effective and reliable use of JACCS using a laptop computer interface, the user requires a higher-end system, and a rugged case may be required in certain tactical environments.

## Warfighter Impressions

- User friendly; great system which works well.
- Timely use of Web browser facilitates fire support coordination.
- Bandwidth management at lowest echelons a warfighter consideration.

**Sponsor:** Mr. Chris Fardell, Air Force Communications Agency (618) 256-2658



### Description

- Provides GCCS and TADIL-J data on 3D stereoscopic rendering of the battlespace.
- Provides innovative interaction devices to provide the CJTF and component commanders enhanced awareness of the battlespace and ability to:
  - Change viewpoint.
  - Filter scene to show items of interest.
  - Display the history of any track(s).
  - View the situation either in real-time or use rapid replay and review capability.

### Capability Assessment

- Provided a fused real-time, 3D stereoscopic representation of the battlespace (e.g. friendly, enemy, and neutral air, land, surface and subsurface) track data.
- Provided the commander/decision maker and operator the ability to change the 3D battlespace presentation using speech commands. Uses input devices to control battlespace point and distance view, select and filter displayed tracks, and hook tracks for more information, zoom and pan, select rate of replay, and toggle monoscopic vs. stereoscopic display.
- The demonstration constantly accepted broadcast track/event data from GCCS COP and TADIL-J.

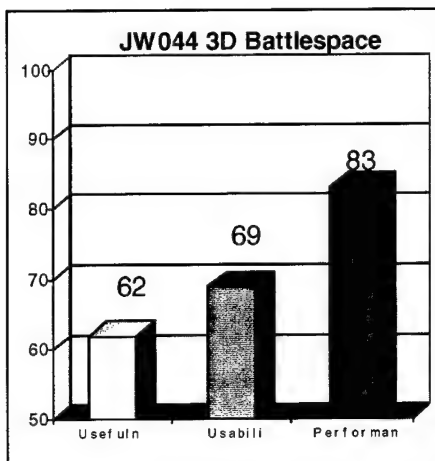
### Objectives Supported

Objective 3 - Met one of the technical challenges by providing a fused, near real-time, true representation of the Warrior's battlespace in 3D.

Objective 6 - Used COTS/GOTS technology to provide constant data exchange of track to deployed elements of the CTF.







## Quick Look

Provided continuous stereoscopic display of all tracks with the ability to change viewpoint, filter icons or tracks, show track history, and replay the situation at desired speed. Evaluation performed at sea during underway operations.

## Results

**Usefulness – 62%:** The demonstration did not receive all inputs directly nor filter track data. Initially the system software did not display all tracks.

**Usability – 69%:** The display zoomed and panned smoothly with both the joystick and with voice commands. The system was easy to learn and manage. Most evaluations stated that the system was technically impressive, however, more work was required to integrate decision aids to quickly tailor the display.

**Performance – 83%:** The system was reliable, both at fixed locations and at sea.

## Value Added

There were mixed evaluations from warfighters and operators. Opinions ranged from “the 3D display reduced command decision times” to “the display offered no warfighter utility in decision execution”. The positive comments included the ability to play back events in a compressed timeframe, rehearsal ability, potential to be used as an interactive planning tool, and an excellent briefing tool. Negative remarks included that the display was only marginally better than existing 2D and 3D presentations and that the size of the display made it impractical for tactical or field applications.

## Conclusions

This emerging technology is not ready for field use but has potential and should be further developed. The system has been installed at the JTASC/JBC and CC Seoul.

## Recommendations

- Continue development of this emerging technology.
- Enhancements should include: reduction of overall size and space requirement, additional filters for declutter, full use of mil standard and symbolic symbology, and full integration with information sources, and integration with other battlefield situation awareness tools to aid in decision making.

## Warfighter Impressions

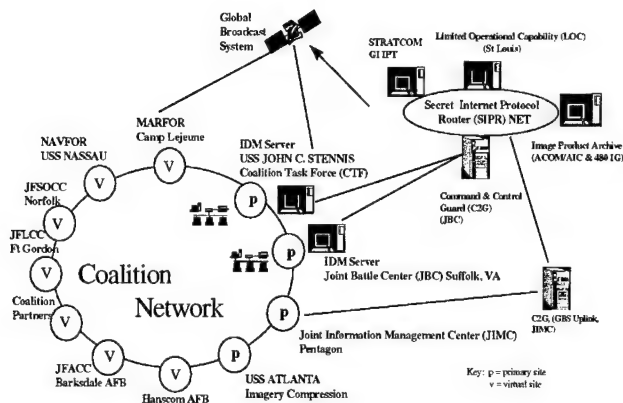
- System was easy to learn and manage.
- The 3D presentation reduced decision timelines.
- Play back capability in compressed timeframes a plus.
- An excellent briefing tool.
- No utility as an execution tool and little added value over existing systems.
- Size is a disadvantage in a tactical environment.

# JW-045 Imagery and Geospatial Support (I&GS)

**Sponsor:** Tony Szalkowski (703) 808-0844, DSN 898-0844, szalkowska@nima.mil

## Description

- Provides on demand Warfighter access, delivery, retrieval, and operational use of USIGS Imagery and Geospatial Information.
- Accesses and uses information via any PC or UNIX-based workstation capable of running web browsers and applications.
- Updates information via NIMA and tactical input from the warfighter and makes it available on a server.



## Capability Assessment

- Imagery and Geospatial Support provided warfighter access, delivery, retrieval, and operational use of United States Imagery and Geospatial System (USIGS) imagery, imagery intelligence, and geospatial information on demand.
- Participants were able to access and use information via any PC or UNIX-based workstation capable of running web browsers and applications.
- Information was updated via NIMA and tactical input from the warfighter, and made it available on a server.

## Objectives Supported

Objective 1 - Imagery and geospatial data were transferred to the coalition WAN from the SIPRNET via the Information Dissemination Management (IDM) server and Command and Control (C2) Guard.

Objective 2 - The COP and imagery could be viewed at any site connected to the CWAN. The COP could be viewed via a link with GCCS, and the source of imagery and geospatial data was transparent to the users.

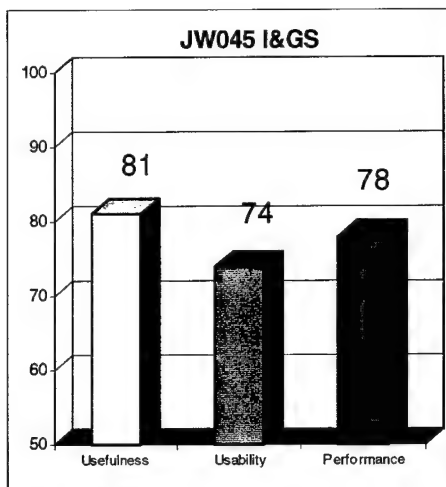
Objective 3 - EDGE application Menu/Graphical User Interface (GUI) was easy to use and system response times were good.

Objective 4 - The concept of providing images to the warfighter for program planning was demonstrated. Using the EDGE application, images could be geolocated on charts and overlaid with various environmental conditions like weather or infrared (IR) simulation. Demo images were synthetically generated which lacked corner coordinates for accurate geolocation.

Objective 6 - The IDM server and C2 Guard architecture provided NITF imagery and geospatial information with updates to all sites connected to the CWAN via an image viewer on the web browser.







## Quick Look

[illegible]

## Results

**Usefulness – 81%:** This demonstration allowed incorporation with common operating picture systems without having to manually manipulate the data. The value of updated imagery and geospatial data during any crisis or event would be extremely beneficial.

**Usability – 74%:** I&GS and the EDGE Menu/GUI was easy to use except for the product information window and the procedures for accessing imagery from other UNIX & PC workstations.

**Performance – 78%:** All information provided was timely and available on one system. I&GS reduced the amount of time spent working on products to support strike planning and enhanced the ability to provide maps/charts and geospatial support to the Commander.

## Value Added

The IDM and C2 Guard add an important dimension that is presently not available to the user, i.e. the ability to pull imagery and geospatial information from a US-only network to an allied or coalition environment.

## Conclusions

The IDM and C2 Guard capability is presently not available to pull imagery and geospatial information from a US-only network to an allied or coalition environment. Imagery and geospatial data could be accessed from many various sources that previously could only be accessed through a time-intensive process, and only on limited occasions. Access to updated imagery and geospatial data during any crisis or event will enable planners and decision makers to have the capability to quickly view opposing targets or current capabilities. The different Controlled Image Base (CIB) images, NITF images, vector data, and other geospatial products enable the warfighter to view the scene minutes prior to the mission.

## Recommendations

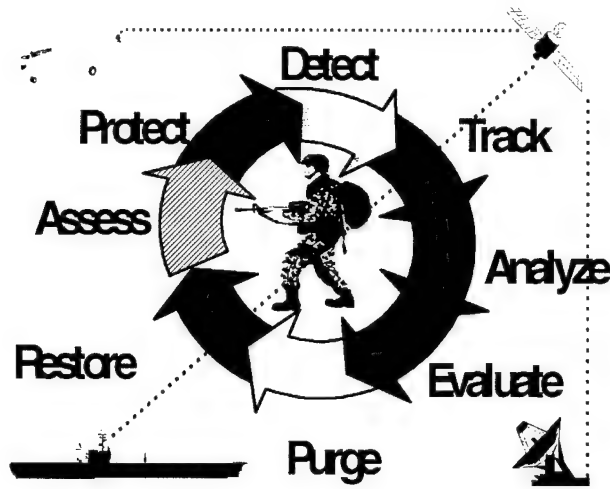
- Field the system now. Incorporate a compression engine. Improve the “product information” window.
- Enhance the procedures for accessing imagery from other UNIX and PC workstations.
- Incorporate message indicator for location and file size of information being requested.

## Warfighter Impressions

- Would take this system/ capabilities to the field now.
- Mission could not be performed without this capability.
- As an imagery analyst, could not perform my task without this system in a coalition environment.
- Difficult to control all data being drawn from the NIMA pipe without C2 Guard.
- Imagery and Geospatial Support is ready for use.

# **JW-052 *Information Operations (IO) Defense and Information Battle Damage Assessment (I-BDA)***

**Sponsor:** Michael H. Shank, Delfin Systems (703) 518 0260 mshank@east.delfin.com



## **Description**

- Provided enhanced information operations defense and battle damage assessment for the Coalition warfighter.
- Integrated real time monitoring and detection (ASIMS) with innovative automated assessment tools (ACES).
- Value added by defense of info systems through the synergy of early detection, automated detailed analysis, and focused deterrence.

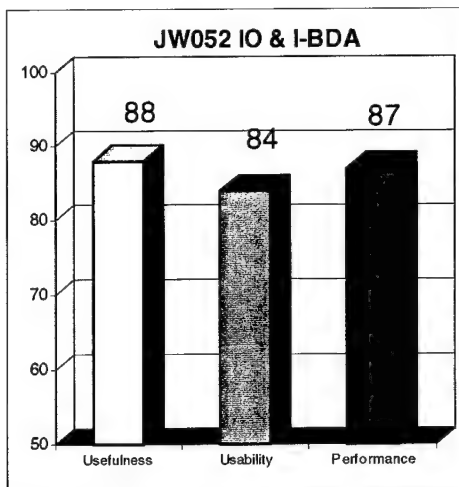
## **Capability Assessment**

- Information Operations (IO) Defense and Information Battle Damage Assessment (I-BDA) demonstrated the ability to detect, analyze, and defend against offensive IO. It used the Automated Security Incident Measurement (ASIM) device to detect unauthorized intrusions, the Automated Computer Examination System (ACES) to track, analyze, and determine the nature and extent of the intrusion, and the ENVOY visualization tool to integrate ASIM and ACES data.
- The software system detected unauthorized activity. Once activity was detected, the system was able to track, analyze, and determine the nature and extent of the unauthorized activity.

## **Objective Supported**

Objective 5 - Immediately notified the user of intrusion and provided a graphic display from which trained personnel could determine which areas were attacked, and make an assessment of damage to permit development of countermeasures. Information Warfare alert messages were disseminated to Coalition forces as part of scenario events, and the system was able to lock out intrusions on subsequent attempts.





## Quick Look

- ASIMS detected unauthorized activity and alerted the operator.
- ACES provided the ability to track, analyze and determine the extent of the intrusion.
- ENVOY provided a easy-to-use presentation of the indicators and analysis.
- Intrusions were directed only to the specific IP address where ASIMS was loaded.

## Results

**Usefulness – 88%:** The integration of ASIM and ACES through ENVOY allowed the visualization of data from two proven intrusion detection tools to simplify the analysis process.

**Usability –84%:** The information was accurate and the level of detail could be tailored so as to begin intrusion assessment at a high level and then focus down to areas of particular interest.

**Performance – 87%:** The system was consistently able to identify the intruded files and begin damage assessment.

## Value Added

This demonstration provided defense of information systems through early detection, notification, damage assessment, and the ability to lock out subsequent intruder attempts. The primary value-added was the integration of ASIM and ACES through ENVOY, providing an easy, yet complete view of the nature and extent of intrusion.

## Conclusions

The ASIM, ACES and ENVOY software provided an easy and complete IW capability which could be used at various network levels. The presentation was easy to understand and intrusion analysis could be done with relatively little additional training.

## Recommendations

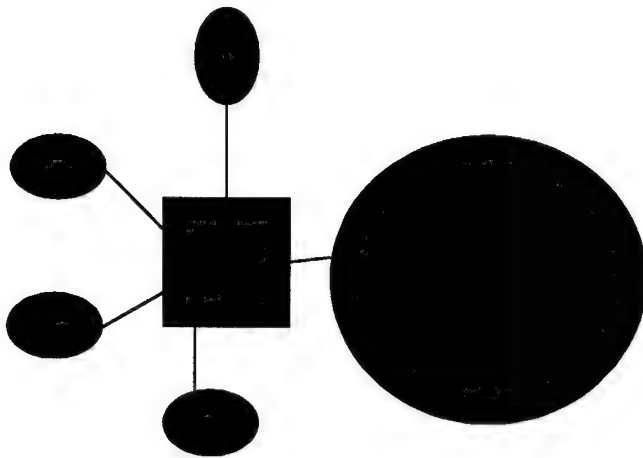
- Evaluate the integrated elements of this system (ASIMS, ACES and ENVOY) in a more realistic operational environment to verify the findings of JWID 97.
- After post JWID JBC verification, field to Warfighter networks.

## Warfighter Impressions

- A complete system with intrusion detection, operator/system manager alert mechanism which can analyze and document intrusion activity and provide intrusion deterrence.
- Easy to understand and comprehend.
- Would like to see in a more realistic environment.
- Could use now.

# JW-060 *Trusted Coalition Scenario Data Base (TCSdb)*

**Sponsor:** Cheri Reed, 301-907-2364, creed@us.oracle.com



## Description

- Provides the coalition with a consistent, real-time view of the battlespace that contains pertinent data.
- Proves coexistence and migration can occur between trusted and non-trusted technologies.
- Provides reduced cost of operations for C4ISR solutions by producing applications which are less complex to create, free of application-level security overhead, and have a much lower life cycle cost.

## Capability Assessment

- The application provided a consistent real-time picture of the battlespace across the coalition.
- The designated user was able to downgrade data to the coalition releasable level which was automatically replicated and shared across the coalition.
- The capability to enhance real-time situational awareness information transfer and downgrading requirements between US and coalition forces provided by this demonstration was valuable.

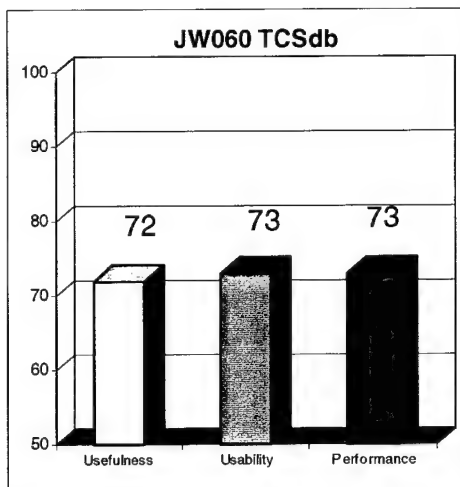
## Objectives Supported

Objective 1 - Provided a concept to provide real-time and seamless information exchange between multiple levels of security at the Coalition Task Force (CTF) and component level.

Objective 5 - Validated that data can be made available and kept secure from unauthorized access through the use of coalition partners accessing the TCSdb at different levels of security.

Objective 6 - Demonstrated the ability of commercial off-the-shelf/government off-the-shelf (COTS/GOTS) technology to provide constant data exchange with deployed elements of the CTF.





## Quick Look

- Classified data was downgraded to the coalition releasable level and shared with coalition database
- Has valuable tool potential for shared information between US and Allied/Coalition Forces with varied security authorizations
- Data provided enabled warfare commander to make real-time decisions
- Database replication was demonstrated

## Results

**Usefulness – 72%:** This system has the potential to improve coalition force data connectivity, but needs further development prior to fielding. Demonstration provided a capability to access information and protect data from unauthorized access and is most suited for use at the JTF/CTF level for information flow. The data fields for the TCSdb were not sufficient to obtain all information provided through the database.

**Usability – 73%:** Replication was successful, though a database manager is required to insure complete and correct transfer.

**Performance – 73%:** Database replication between JBC, SHAPE and the USS John C. Stennis was demonstrated; an allocated IP address was required to connect with the other JWID systems.

## Value Added

TCSdb has excellent potential value added for US/coalition operations. TCSdb provided a single source database enabling coalition members to input information to a common database.

## Conclusions

Use of a real world database with varying data elements for sanitizing/downgrading purposes should be used to fully demonstrate the TCSdb capabilities. It has valuable tool potential for shared information between US and allied/coalition forces with varied security authorizations. Provided a proof of concept for authorized declassification and release of information deemed important for coalition members.

## Recommendations

- Enhance capability to access data in the database to allow sanitization.
- Provide the ability to downgrade all levels of classification.
- Develop CONOPs to manage replicated databases.
- Better define the consistent real time picture of the battle space that TCSdb provides.

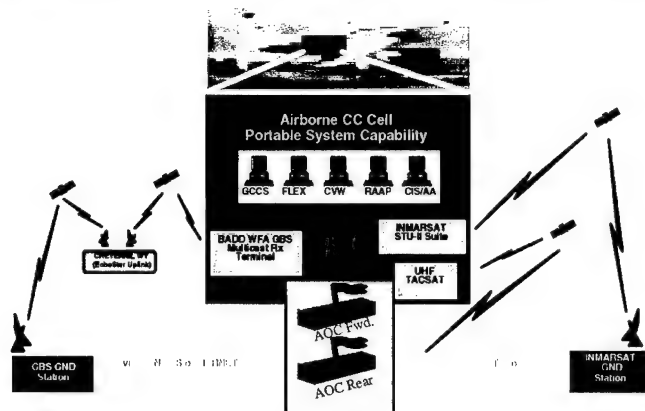
## Warfighter Impressions

- Functional shortfalls indicate that the system is not ready for the warfighter.
- With more development, TCSdb should provide a powerful tool.
- Warfighter's inability to manually change, delete offending data or successfully downgrade information reduces value.
- TCSdb has potential to save time and eliminate coalition sharing of information but, additional work is required.



# **JW-068 *Deployable, Distributed Joint Force Air Commander (JFACC) With Airborne Command Cell***

**Sponsor:** LtCol. Barbara Wagner, ACC/SMO-V, wagner@hqacc.langle.af.mil, DSN 574-8800



## **Description**

- Provides distributed, collaborative planning, and near real-time situational awareness.
- Supports geographically separate AOC Rear and Forward locations, as well as in-transit JFACC staff.
- Uses DISA GBS, DARPA BADD, and Speckled Trout to accomplish this AF initiative.

## **Capability Assessment**

- Provided real-time collaboration between planning cells at dispersed locations for Air Tasking Order (ATO) generation. Deployable, Distributed (DD) JFACC allowed the generation and use of Intel data, Target Nomination Lists (TNL), ATOs, and mission status between Air Force and Allied planners at geographically dispersed locations. Airborne JFACC, in near real time, made recommendations to ground based Air Operations Center (AOC) planners for high priority targets to be incorporated into next day's ATO.
- Forward Eagle (FE) provided situational awareness for JFACC in transition from AOC Rear to AOC Forward.
- Battlefield Awareness and Data Dissemination (BADD) delivered tailored information, including imagery, to display a COP on the warfighter associate display.
- The Collaborative Virtual Workspace (CVW) enabled near real time planning between AOC Rear and Airborne command cells and between AOC Rear and AOC Forward.

## **Objectives Supported**

Objectives 1 and 5 - Did not exchange information between multiple levels of security. Collaborative planning and ATO generation were accomplished with Coalition Forces, at the coalition access level.

Objective 2 - Used GBS and BADD information management. Supported wide-band communication capabilities to the Speckled Trout aircraft while inflight for near-real-time situational awareness and collaborative planning.

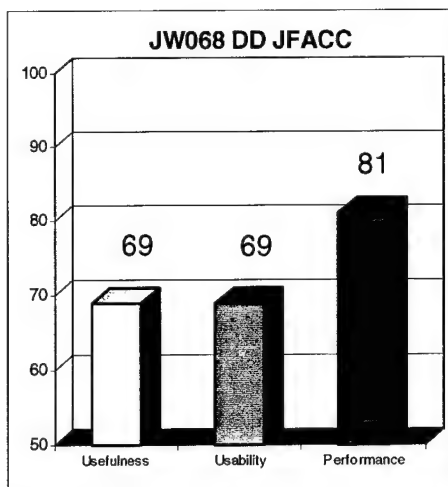
Objective 3 - Demonstrated distributed situational awareness and planning capability for Coalition Task Force and air components.

Objective 6 - Provided integration of predominately COTS and GOTS based systems and tools which provided support to distributed JFACC planning and execution capabilities. It also included a phased array antenna used to receive wide-band communications on the Speckled Trout.

Objective 7 - Demonstrated enhanced collaborative tools and information management which will enable further evolution of the DII COE as a core infrastructure for DOD information systems.

Objective 8 - Did not demonstrate tracking of logistics resources, but wideband communications and information management capabilities demonstrated would be indicative of the reachback capability.





## Quick Look

- CCTF on USS John C. Stennis conducted VTC with in-flight JFACC transitioning to AOC Forward.
- Accomplished collaborative ATO generation between AOC Forward, AOC Hear, Canada, and Hanscom.
- Demonstrated capability to provide situational awareness to airborne JFACC (BADD/WFA).
- CVW provided useful tool for planning and monitoring operations.

## Results

**Usefulness – 69%:** For its demonstrated function, the D/D JFACC provided complete information access, however, the CONOPS will have to address access to information for the full planning function as much of the information required, under operational conditions, is at special access security levels. Operators were able to perform collaboration with components at AOC locations, the Airborne JFACC, and CCTF using CVW.

**Usability – 69%:** Operators found the system easy to use. The weaponeering options entered into Rapid Application of Air Power (RAAP) were not consistent with the Airspace Deconfliction System (APS), so the TNL downloaded with errors making the weaponeering options unstable. There was no ADS so that the airspace data was not pulled as would be the normal course of action.

**Performance – 81%:** Considered good after the first week. In addition, system failures by the Joint Planning Tool (JPT) and unreliable connectivity with the CVW server at Hanscom led to a decision to stop the demonstration until the beginning of scenario phase two.

## Value Added

The value added was the ability to perform distributed air battle planning and air tasking order generation, and to support situational awareness aboard the airborne platform during JFACC transition. CVW provided a means of collaboration which would allow real-time interaction among planning staffs.

## Conclusions

CVW provided great collaborative capabilities, however, some reservations were expressed about proliferation and interoperability of collaboration tools. The capability to implement a distributed AOC requires a CONOPS for this structure and there is concern that the distribution would foster a return to service unique AOR implementations and increase vulnerability to information warfare (IW).

## Recommendations

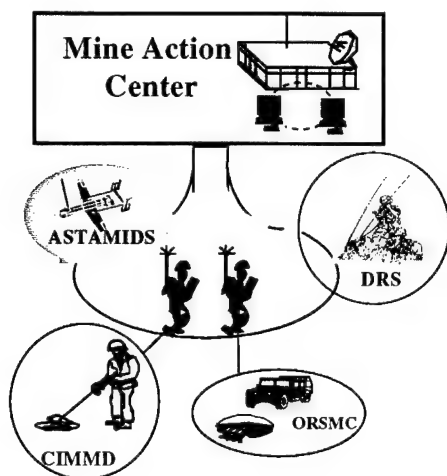
- Continue development and acquisition of BADD/WFA for improved airborne situational awareness.
- Develop concept of operations for the Distributed AOC and test with a fully capable planning cell.
- Reduce the number of unique and incompatible collaboration tools and field only a common tool and include in the DII COE.

## Warfighter Impressions

- Requirement to operate up to 16 different menus to conduct planning untenable.
- JPT software requires maturity to be useful.
- System provided redundant features already in the field.
- Inability to run CVW and RAAP drastically affects operation.
- UNIX background operating system mandated continued contractor actions.
- Help screens needed to facilitate operator continued operations.

# **JW-073 Joint C4 for Intelligence Surveillance and Reconnaissance (C4ISR)**

**Sponsor:** Mr. Barry Blumenthal, JCM ACTD Joint Program Office (703) 696-6943



## **Description**

- Provide Joint and Coalition commanders the tools to effectively plan JCM operations, monitor, and evaluate situations, and control JCM forces and systems.
- Exchange near real-time collaborative planning, and situational awareness about mines.
- DII COE compliant technology.
- JCA and web-based browser user-interface programs to plan countermine operations.
- Use of VMF, USMTF and other message sets using MLS bridges.

## **Capability Assessment**

- Joint Counter Mine (JCM) exchanged near real-time collaborative planning, Situational Awareness (SA), releasable ISR sensor and minefield information between US and Joint forces.
- JCM allowed planning between countermine operations and maintains JCM COP SA.
- JCM exchanged data between the individual warriors in the field and the CJTF and Components.
- Tailored JCM COP data and imagery from national tactical reconnaissance minefield/booby traps obstacles were sent/received by the individual warrior.
- JCM provided the capability to develop, maintain, and disseminate integrated tactical picture.

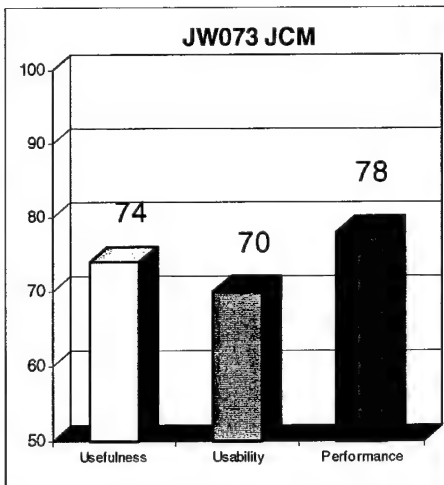
## **Objectives Supported**

Objective 1 - Showed the ability to exchange real-time information at multiple levels of security using the RADIANT MERCURY MLS gateway (using HP Series 700 servers).

Objectives 2 and 6 - The GCCS/JMCIS/TCO systems were all developed from commercial Sun workstations and the DII COE built up into a full GOTS software suite.

Objective 3 - Demonstrated tailorable situation awareness through fusion of ISR, force assets, and mine/minefield data.

Objective 7 - The JCM builds on top of the DII COE and provides additional countermine functionality. The scenario for this demo did not stress the system to validate its reliability and worthiness to be included in the COE. The demonstration did show the ability to communicate via the CWAN using the RADIANT MERCURY server. The communications from the JMCIS to NT PC was validated. Enhancements to warplanning operations were provided by access to various imagery, intelligence, and other information displayed by the Netscape browser, a client of the NT PC architecture.



## Quick Look

- Exchanged near real-time collaborative planning and situational awareness (ISA) sensor and mine field information between US and Allies.
- Allowed planning between coalition mine operations and maintainers (JCM COP, SA).
- Exchanged mine information and data between individual warfighters in the field and the JTF.
- Tailored JCM COP data and imagery from National Minefield Policy (NMP) sources were sent to the warfighter.

## Results

**Usefulness – 74%:** Provided the capability to develop, maintain and disseminate an integrated tactical picture and the COP for a comprehensive JCM common mission planning tool. Demonstrated the ability to distribute mission results to commanders in a timely manner. Provided JCM information to small units down to the HMMWV level. Plotted mines, provided imagery, and facilitated the transmission of OPNOTES between warfighters for collaborative planning.

**Usability – 70%:** After receiving sufficient training, the JCM systems mission planning tools were easy to use. The system screens were much easier to use than compatible systems. The warfighter commented on how easy it was to plot, send, and track mine fields, assets and contacts in the field. There was a problem with font and icon size that resulted in operator misunderstandings.

**Performance – 78%:** The system was operational approximately 75% of the time due to system lock-ups. The JWID scenario did not properly stress the system to validate its reliability.

## Value Added

The JCM demonstrated a system that provided all levels of command the ability to view the JCM COP and SA information. It allowed use of the JCM information in both planning and executing Joint and Coalition operations. It provided the ability to supply a joint battlespace picture of both land and sea mines for coalition forces. It provided the capabilities to integrate imagery, intelligence sources, and real-time communications to produce a JCM COP.

## Conclusions

The warfighters evaluated the system as providing a needed capability, however, this demonstration was not designed to provide a total test of the system. The overall consideration is that the system still needs additional tuning prior to fielding or final testing.

## Recommendations

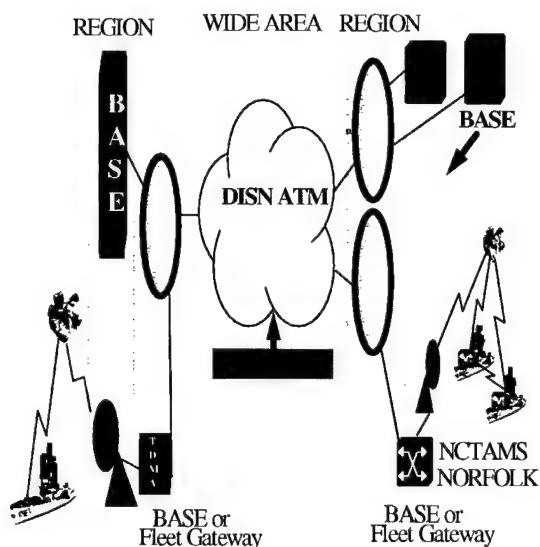
- Additional integration is necessary in order to use this system in other than a naval environment.
- Requires automatic system reference number assignments to mines and ability to set default values.
- Add current sonar packages to best utilize the JCM capability.
- The system must be further tested under a stressed scenario.

## Warfighter Impressions

- Detailed mine hunting info is displayed and condensed into mine dangers for transfer to the COP.
- Provides a joint battlespace picture of both land and water mines.
- Very complicated to learn.
- Based on naval operations and lacks detail necessary for land operations.

**JW-074** *Joint Maritime Communications (JMCOMS)*

**Sponsor:** Mr. Mike Davis, (619) 503-1819



## Description

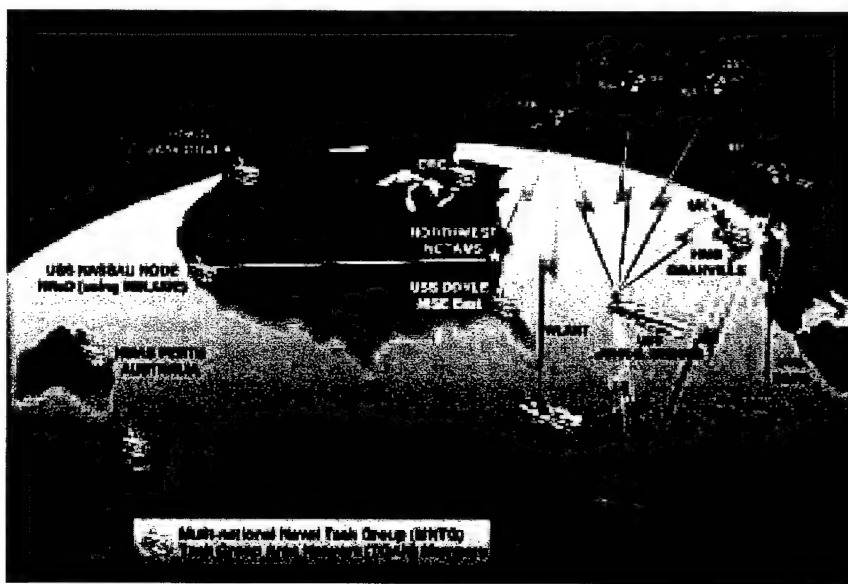
- Enhanced commercial full duplex T-1 link SATCOM terminal (Challenge Athena III).
- New advanced UHF waveform tested in MINI-DAMA unit that will double UHF SATCOM; used TCP/IP over UHF SATCOM to a submarine.
- Enhanced maritime info exchange to Joint/Allied forces and improved C3 effectiveness and interoperability using IP networks along with X.400 messaging, multicasting, and receipt of X.400 traffic in EMCON (TGAN).

## Capability Assessment

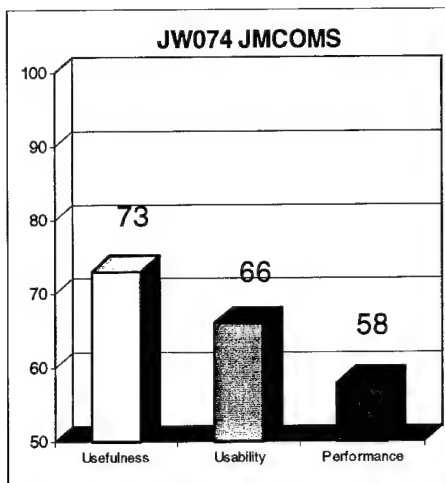
- Automated Digital Network System (ADNS) provided connectivity for tactical information exchange with each participating platform functioning on the SIPRNET and CWAN.
- JMCOMS demonstrated the Digital Modular Radio's advanced UHF waveforms RF transmission capability supporting the Internet Protocol (IP)/ADNS communication connectivity.
- Multi-National Naval Task Group (MNTG) demonstrated the capability to support multicast with ships over existing bearers, provided X.400 messaging to and from mobile units over existing bearers and demonstrated successful receipt of X.400 traffic by ships in Emissions Control (EMCON), and demonstrated the exchange of track data between Allied units and Joint and Combined forces using IP Networks.

### **Objectives Supported**

Supported objectives 1, 2, 3, 5, 6, 7 and 10. The primary objectives for this demonstration were 2 and 7, which deal with new, innovative telecommunications technologies and enhancements to the DII. New technologies that were demonstrated included MINI-DAMA which provided increased bandwidth to submarines from 16 to 38.4 Kbps using new waveform, Challenge Athena which provided enhanced throughput with commercial SHF SATCOM by increase of receive only 368 Kbps to full duplex 1.544Mbps, and Task Group Area Network (TGAN) which provided 400 messaging and services in the MNTG.







## Quick Look

- MINI-DAMA provided increased bandwidth to submarines using new waveform.
- Challenge Athena provided enhanced throughput with commercial UHF SATCOM.
- TGAN provided X.400 messaging and services in the Main National Naval Task Group (MNTG).
- Increases in bandwidth and X.400 features provided a significant increase in capability.

## Results

**Usefulness – 73%:** Demonstrated technology insertion with enhanced throughput for submarine and task group communications. This technology insertion also included multicast, X.400 messaging between mobile units, and message receipt during EMCOM which significantly increased the effectiveness of network centric operations, and has wide-ranging joint and coalition applicability.

**Usability – 66%:** Ship communications personnel found the equipment easy to use. The MINI-DAMA and MD-1324 modem training was endorsed by the operators. TGAN operators were able to connect to the IP network and use it, but reported long waits caused by the 16Kbps data rate.

**Performance – 58%:** All JMCOMS systems on the USS John C. Stennis were available. TGAN network availability was impacted by satellite resources availability which reduced operating time to two-five hours a day.

## Value Added

The use of commercial satellites adds to the robustness of military SATCOM systems, and the advanced UHF waveform doubles UHF SATCOM throughput. Internet protocols and connectivity (TCP/IP) to submarines using MINI DAMA terminals over DAMA UHF SATCOM resulted in the first use of TCP/IP interconnectivity over that medium to submarines. TGAN increased the effectiveness of MNTG operations by providing tracks, and an audio teleconferencing capability. The MNTG used Communications Systems Network Interoperability (CSNI) and ADNS technology to send 123/X.400 messages to exchange the COP and plan operations collaboratively.

## Conclusions

JW074 has potential to facilitate the network-centric operations necessary for modern warfare, including: commercial wideband satellite systems that are reliable assets for CTF Component and Allied commanders; an advanced UHF waveform that doubles throughput for all services using UHF SATCOM channels; MINI-DAMA terminals using TCP/IP protocols between ships and submarines; and TGAN, providing multicast, X.400 messaging, and message receipt during EMCOM.

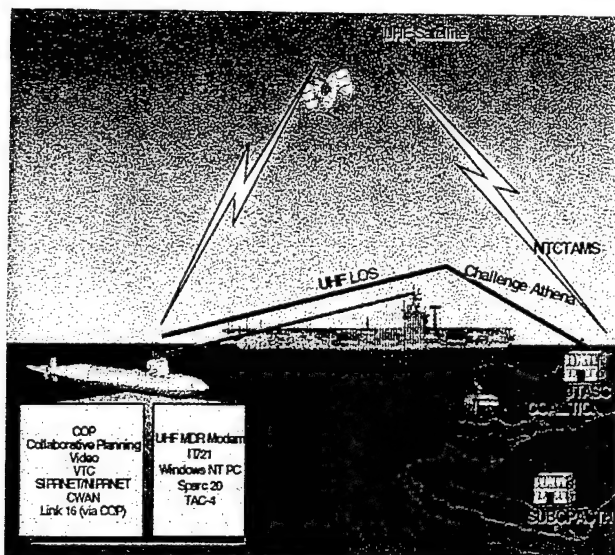
## Recommendations

- Expedite network-centric operational testing to fully exploit internet connectivity to mobile platforms.
- Continue development and use of advanced waveform.
- Continue development of TGAN capabilities to satisfy network protocol requirements.
- Expedite the phased Navy fielding of this technology.

## Warfighter Impressions

- Operators found the commercial SATCOM equipment user friendly.
- Database interoperability and interaction between other sources of information was impressive.
- Increased bandwidth to the Submarine received many positive comments as to potential warfighting utility.

Sponsor: Captain William W. Matzelevich, N872E; phone: (703) 697-1999; matzelevich.william@hq.navy.mil



## Description

- Combines a submarine's inherent stealth, mobility, and firepower with the capability to be a full real-time participant in the COP and integrated sensor-to-sensor and sensor-to-shooter technologies.
- Provides a network architecture and greater bandwidth access to significantly increase sub accessibility to commanders.
- First time participation in collaborative planning, tactical VTC, and COP.

## Capability Assessment

- The UHF LOS data link operated at 512 Kbps TCP/IP in full duplex mode.
- The data link supported the Telemedicine capability by transmitting medical images to consulting physicians.
- The data link supported the strike planning/collaborative planning by allowing the coordination of strike plans with CJTF staff and other exercise elements.
- Special Warfare Automated Mission Planning System (SWAMPS) provided a first time capability for operational collaboration between CJTF, Joint special Operations Task Force (JSOTF), and Special Operations Forces (SOF) embarked on a submarine during at-sea operations.

## Objectives Supported

Objective 2 - Provided enhanced data delivery between ships and submarines at sea.

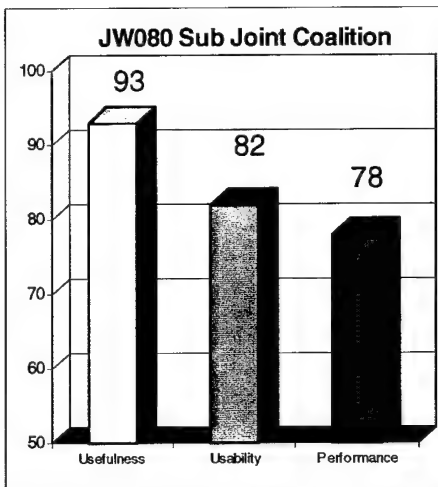
Objective 3 - Contributed to dominant battlespace awareness by supplying operational information using the COP and imagery transfer over the SIPRNET and CWAN. Early in the Deployment Phase, the submarine passed periscope imagery of high interest contacts, piloted Unmanned Aerial Vehicles (UAVs), passed tactical data, and mapped minefields using Unmanned Under-water Vehicles (UUVs).

Objective 4 - Full network connectivity in COP and NWCS architectures. Provided real-time targeting information to Joint Intelligence Center (JIC)/CJTF Strike Cells using organic submarine sensors.

Objective 6 - Supported the constant data exchange of medical images between the Submarine and Atlantic Fleet Undersea Medical Officer, the Battle Group Medical Officer, and the Senior Medical Officer at Bethesda Naval Hospital. SWAMPS demonstrated the ability of COTS software to support mission planning for special operations (Seals).

Objective 9 - Promoted integrated single computer operations through economized PC use, common software applications on workstations, and developed time sharing schemes to accommodate submarine footprint.





## Quick Look

- Integrated available C4I technology to significantly improve sub interoperability in support of joint and coalition force operations.
- Full participation of networks.
- Improved treatment/disposition of warfighter patients by enhanced communication with physicians at low cost \$12K COTS product.
- Ability to perform telemedicine.
- Fully integrated and reduced planning time for SWAMPS operations.

## Results

**Usefulness – 93%:** Telemedicine provided detailed images in a timely manner. SWAMPS also provided a collaborative and information access capability that greatly reduced the time for mission planning. Information was able to be shared among the battle group so that medical experts at various locations could view medical imagery, data, and provide feedback to the submarine on possible courses of action.

**Usability – 82%:** Operators reported that both the Telemedicine system and SWAMPS were easy to use with a minimum of training.

**Performance – 78%:** The Telemedicine system provided information and pictures that were immediately available to several medical facilities simultaneously. SWAMPS capabilities were available except for some initial communications outages experienced on the CWAN and the SIPRNET.

## Value Added

The Telemedicine system provided submarine Independent Duty Corpsmen (IDCs) access to medical expertise not previously available to a deployed underway submarine saving time and potential lives. SWAMPS was used to conduct post mission intelligence briefings to the CCTF on USS John C Stennis from the Seals on USS Atlanta using the SWAMPS' tactical VTC capability while operating at sea. Whiteboard, Chat Box, maps, imagery, and charts were used to show the specific locations of mines and water obstacles in real time.

## Conclusions

The Telemedicine system demonstrated medical capabilities and expertise not previously available to IDC's without diverting or canceling the operational mission. SWAMPS provided a wide range of functionality in its current form. The package is still new and requires further study. It provides some generic capabilities that may be useful to other tasks beyond mission planning. The essential feature of JW080 that supported both Telemedicine, SWAMPS and the other demonstrations hosted on board USS Atlanta was the equipment and associated network architecture that permitted high bandwidth data transfer with USS John C. Stennis.

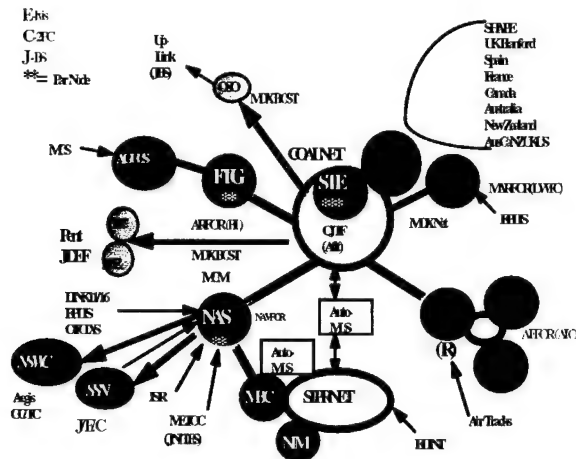
## Recommendations

- Examine required doctrinal changes to provide submarines and other tactical units with demonstrated bandwidth and network access.
- Field essential telemedicine capabilities to submarines and investigate its use at other tactical units with limited medical facilities.
- Field imagery portion of system.

## Warfighter Impressions

- Provided IDC medical expertise not previously available.
- Provided timely detailed images.
- Telemedicine reduces the need for MEDEVAC to another ship.

**Sponsor:** CAPT Gerald Nifontoff, USN. SPAWAR PD18, (619) 524-7651



## Description

- Provides the COP.
- Integrates ISR data and METOC data into the COP.
- Provides ISR sensor management and sensor performance assessment tools to support improved situational awareness, mission planning and tasking.

## Capability Assessment

- The ISA provided new retrieval, display, and distribution capabilities, which include: a) tailorable COP with filtering and compression to submarines and other low-bandwidth units, b) introduction of enhanced display of the Ground Order of Battle highlighting the new Enhanced Position Location Information System (EPLIS), c) a battlefield roll-up and spread display option to view multiple small land units, a) a C2PC to distribute COP to PC users at both LAN and WAN sites using the C2PC gateway, and d) ELVIS II COP browser enhanced with a JAVA display and collaborative training capability.
- The ISA provided improved ISR sensor management and performance assessment tools, which include: a) access to JSTARS and Predator Video, b) the ability to link ISR assets/functionality together into a system, c) the ability to display sensor coverage maps and performance assessment for blue force and national sensors, d) an enhanced air picture which automatically ties capabilities and performance data to current air tracks, e) Sensor Status Reporting System providing increased functionality and implementation, and f) a dedicated TMD warning capability from Air Force Space Warfare Center to the Task Force.
- Upgrade to the Joint METOC Segment (JMS) of the GCCS included a user selectable information display on the COP terminal (CWAN only) showing the METOC, impact to operations.

## Objectives Supported

Objective 1 - Aided collaboration and situation awareness to Coalition Forces down to unit level. Files of sensor performance and employment planning were posted to the Trusted Coalition Database via JW060.

Objective 2 - Enabled networking and telecomm solutions through Message Data Exchange (MDX), extended DII COE for operational planning by CJTF, and rapid PLI information dissemination to tactical users.

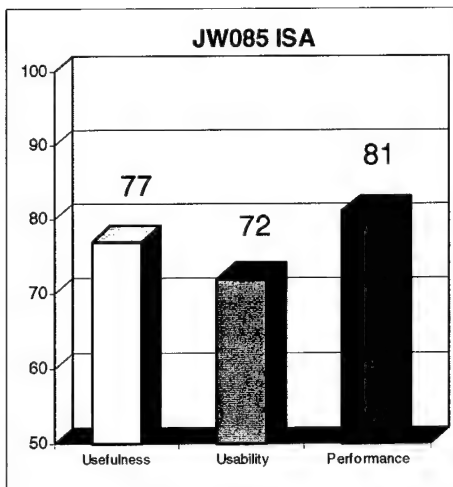
Objective 3 - Provided battlespace awareness by bringing information management and resource allocation to wide range of formerly disjointed stand alone sensors and provided enhanced COP at the CJTF and CC.

Objective 4 - Combat ID was supported with SABER, EPLIS, and TADIL-J sensor feeds.

Objective 6 - Allowed use of web browser technology to provide information to users.

**Objective 7 - The enhanced COP tools and the EPLIS are COE/DII compliant.**

**Objective 9:** The use of the C2PC to receive the COP demonstrated significant use of PC technology.



**Quick Look**

- Tailored COP and delivered that picture to low bandwidth users in a timely manner.
- Integrated SAGE, JSTARS, Predator, TMD warning and METOC data into the COP.
- Sensor management and performance assessment information and the capability to display that information showed potential but lacked maturity.
- Demonstrated capability to display a light version of the COP on a laptop PC.

## **Results**

**Usefulness – 77%:** New retrieval, display and distribution capabilities to the COP were demonstrated. Sensor management and sensor performance assessment information showed potential but lacked maturity.

**Usability – 72%:** The capability to display sensor management and sensor performance assessment information showed potential but lacked maturity. The system was easy to use, with most functions being point and click. Connectivity and interoperability were simple to achieve for most operators.

**Performance - 81%:** The system was reliable and was easily restored when failed or stopped processing.

## **Value Added**

The ISA provided new retrieval, display and distribution capabilities to the Common Operational Picture that significantly increased the situational awareness of the battlespace for the CJTF and the Coalition Forces.

## **Conclusions**

JW085 demonstrated the ability to tailor the COP to selected tracks and geographical areas and provide the picture to low bandwidth users in a timely manner. It also demonstrated the ability to integrate EPLIS, JSTARS and Predator video, TMD warning information, small battlefield unit information, enhanced air track information and METOC data into the COP. A "lite" version of the COP displayed on a laptop PC was also successfully demonstrated. The capability to provide sensor management and sensor performance assessment for coalition forces and national sensors and display that information was demonstrated and found to have potential, but assessed to need more refinement to be of benefit to the warfighter. There were also concerns about the fidelity of the tracks used to create the COP and it was felt that there was a need to have procedures to validate track positions, track fidelity, and overall credibility of the COP. Overall, the Integrated Situational Awareness demonstration successfully demonstrated new retrieval, display and distribution capabilities to the COP that significantly increased the situational awareness of the battlespace for the CJTF and the Coalition Forces.

## **Recommendations**

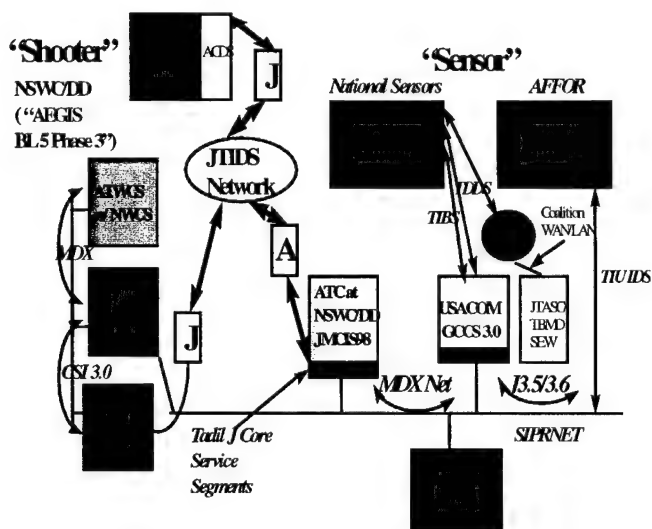
- Refine sensor management and sensor performance assessment tools and the capability to display.
- Develop procedures to validate track positions, track fidelity, and overall credibility of the COP.
- Improve system for joint use by integrating digitized maps and increasing the number of options for development of land forces overlays.
- Include more land military symbols such as lines, arrows, and allow the development and transfer of operational orders.

## **Warfighter Impressions**

- Would have helped us during DESERT STORM.
- Never had this capability and it was confusing from a C2 perspective.
- This system goes a long way toward integrating things needed to accurately grasp the COP.

# ***JW-086 Joint “Sensor to Shooter” Demonstration for TMD, Rapid Precision Strike, and Real Time Collaborative Pre-Strike (RTCPS)***

**Sponsor:** Cheryl Walton, SPAWAR, (703) 602-7157, waltonc@smtp-gw.spawar.navy.mil or CDR Kevin Casey, SPAWAR, (703) 602-1176, casey @nosc.mil



## **Description**

- TBMD displays post-launch multi-sensor correlated missile tracks on the COP and forwards to NWCS.
- RTCPS remote users collaborate using real-time voice, whiteboards, and sensor imagery and sends target data to NWCS.
- TCS controls the UAV/simulator sensor and sends it local imagery and target positions to NWCS.
- NWCS performs target pairing, airspace deconfliction, and fire mission planning and execution.

## **Capability Assessment**

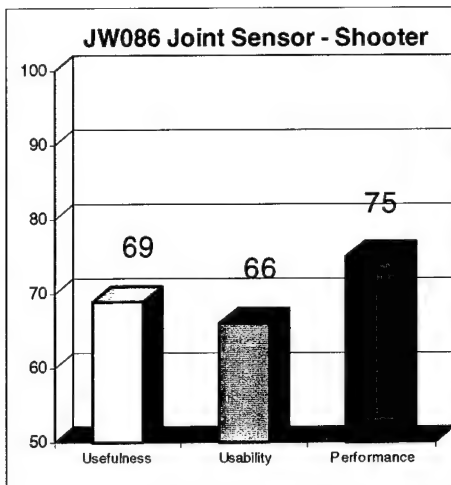
- Tactical Control System (TCS) provided Video and imagery and associated target data to NWCS and others via the Coalition WAN (Live Video, still frames and associated data i.e. target Lat/Long).
- Naval Surface Fire Support (NSFS) Weapon Control System (NWCS) performed target pairing between targets and firing platforms, airspace and space deconfliction between planned fire missions, and fire mission planning for Tomahawk and other munitions.
- RTCPS provided real time voice (via MILSTAR), whiteboard and Imagery (via GBS).
- Theater Ballistic Missile Defense (TBMD) and TBMD Multi-Source Correlator (TMSC) worked together to eliminate redundancies, fuse, and display post-launch missile tracks and send them to the shooter via Radiant Mercury and the COP.

## **Objectives Supported**

Objective 1 - Provided a real time collaborative planning through RTCPS segment. TBMD transmitted alert warning estimated launch positions to NWCS for pre-strike planning and strike execution. Radiant Mercury provided the means for filtering transmitted data.

Objective 3 - Enhanced the JMCIS COP with missile tracks and their launch and impact positions. TBMD received missile tracks from multiple national and theater sensors and dynamically fused and displayed these tracks on the COP. Transmission of TBMD/TMSC data from the JBC to the USS John C. Stennis and USS Atlanta demonstrated tailoring COP data for warfighter use. This was a true sensor-to-shooter sequence utilizing real time updates from the COP.

Objective 4 - RTCPS, TBMD, TMSC, TCS and NWCS interactively connected and completed required sensor-to-shooter sequences.



## Quick Look

- Provided useful intel imagery, targeting tools that reduced mission planning time and helped reduce the sensor-to-shooter sequence.
- RTCPS provided a true collaboration capability to analyze imagery in real-time.
- TBMD/JMCS provided a single integrated launch message.
- Selectable workspaces on the menu bar made it easy to move between applications.

## Results

**Usefulness – 69%:** RTCPS met mission task requirements. The NWCS feature allowed for completion of mission planning tasks. The network capabilities facilitated interaction among sites for distribution of the COP, imagery and intelligence, which provided staff assessors and operators access to information needed.

**Usability – 66%:** The system is easy to operate and its capabilities make completing tasks much easier. The system contributes to the situational awareness being built into the COP for all sites to use. Most of the operators and staff felt they could locate and retrieve information as required with the various systems/segments available to them in the demonstration.

**Performance – 75%:** Once the system/segments stabilized after software difficulties and network connectivity problems, the staff assessors and operators felt the system was available when needed. All the critical functions were demonstrated at some point during the assessment period.

## Value Added

Joint Sensor-to-Shooter provided improved capabilities for the operators and staff to perform their required tasks and missions. They saw potential for the system and felt testing in actual field conditions with the firing platforms were necessary to get further input for modifications and improvements. RTCPS adds significant value to small commands that do not have intelligence analysts organic to the unit. The whiteboarding capability allows collaboration with the experts. The steps in the TCS process of acquiring video were too lengthy. The sponsor stated the connectivity was primitive for JWID and is not representative of the mature TCS system of the future. The ability to control all the services' UAV assets is the real goal not yet met.

## Conclusions

Overall, this is a useful system that needs further testing and evaluation. It provides many useful tools that reduce planning time. NWCS automates time consuming tasks. RTCPS is ready now. TCS requires further development.

## Recommendations

- Further develop system in a test and evaluation environment.
- Base improvements and modifications on actual operator input from the firing platforms, operations centers and imagery sources.

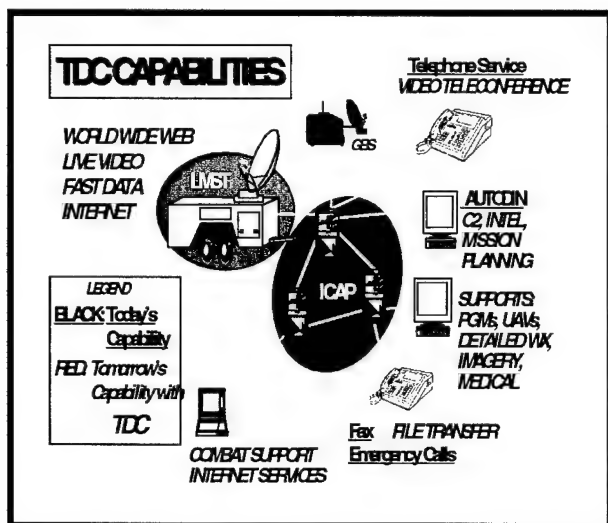
## Warfighter Impressions

- RTCPS capabilities provide value to the warfighter.
- Collaboration with other units on deconfliction of airspace and better defined targets is what you really get with this system.
- The system was reliable.
- Available when needed.



# **JW-089 Theater Deployable Communications (TDC) Support For Deployed Air Operations Centers)**

**Sponsor:** Capt Will Stevenson, HQ ACC/SCCD, Comm (757) 764-6115



## **Description**

- Provides wideband, DII compliant, voice, video, data, and imagery communications for deployed Air Force forces.
- Small, lightweight, modular, and scaleable packages.
- Plug and play commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) equipment.
- Planned for technological growth.
- Interoperates with joint and coalition systems/networks.

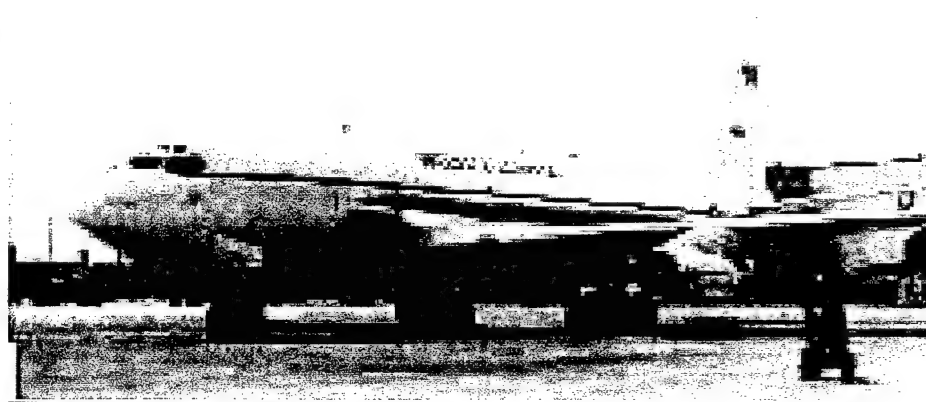
## **Capability Assessment**

- Provided reliable Coalition Network data at 512 Kbps with no evident blockages or outages, reliable SIPRNET data at 256 Kbps with no evident blockages or outages, and reliable NIPRNET data at 192 Kbps with no evident blockages or outages.
- The TDC AOC provided stable and reliable JFACC satellite and infrastructure communications.

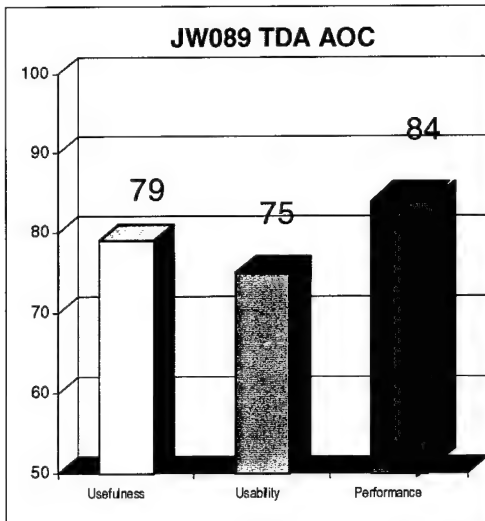
## **Objectives Supported**

Objective 2 - Was unable to meet all of the objective. A production Lightweight Multi-band Satellite Terminal (LMST) was not available for the demonstration due to OT&E. The demonstration used a second channel on the AN/TSC-100A w/Quick Reaction Satellite Antenna for satellite access.

Objective 6 - TDC AOC demonstrated that COTS/GOTS equipment configured properly can support data exchange with in-garrison, in-transit and deployed elements of the Coalition Task Force (CTF).







## Quick Look

- Solid overall in demonstrating comm and data backbone to support the JFACC Forward and CAOC (Voice, CWAN, NIPRNET, SIPRNET).
- Significant reduction in pallet size for air transportation.
- Provided significantly improved capability with smaller operational footprint.
- SATCOM categorized as excellent overall.
- ISDN switch was interoperable at the SF trunk and baseband level, but not at the DTG level with TRI-TAC switching equipment.

## Results

**Usefulness – 79%:** TDC AOC provided the required communications infrastructure. The system allowed interaction between designated users and systems. The Integrated services Digital Network (ISDN) switch was interoperable at the SF trunk and baseband level, but not at the Digital Trunk Group (DTG) level with Tri-service Tactical Communications Program (TRI-TAC) switching equipment.

**Usability – 75%:** Operators found the system easy to use after a few hours of training.

**Performance – 84%:** TDC AOC provided communications via SIPRNET, NIPRNET, and CWAN via the satellite.

## Value Added

TDC AOC provided a combined COTS/GOTS package that was easy for the operators to work with, setup, and configure. It provided reliable voice, video, data, and imagery communications infrastructure to support the JFACC Forward via the satellite. A definite benefit to TDC equipment is a significant decrease in size and weight for forward deployment.

## Conclusions

This combination of COTS and GOTS is a realistic approach to the issues of network accessibility, monitoring, configuration, control and integration of current technology into the warfighters' domain. The VTC over ISDN was demonstrated after the DISA assessment period during VIP week. Although not part of the TDC program, VTC services could enhance the warfighter capability. The COTS and GOTS integration into the TDC AOC demonstration fits right into the path of replacing proprietary, bulky, expensive, and aging technology.

## Recommendations

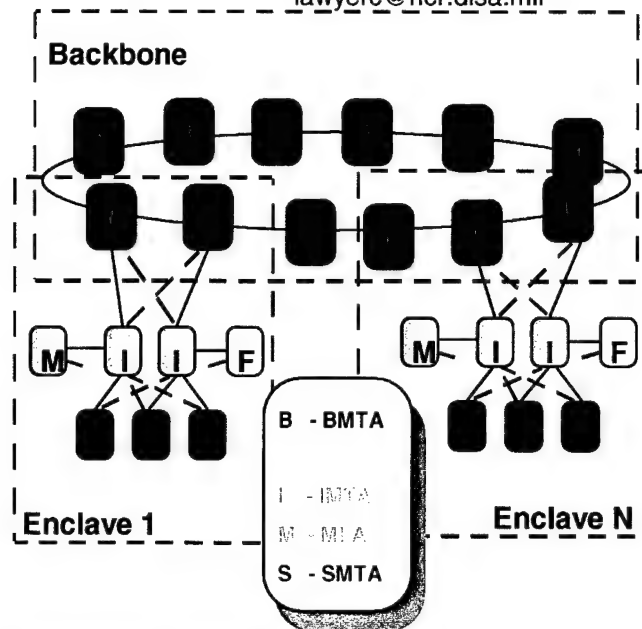
- The program office should identify the specific features and limitations of the TDC equipment to war planners.
- Continue funding this COTS/GOTS approach for theater deployable communications.

## Warfighter Impressions

- Provides reliability in a downsized package.
- Provides a means for incorporating COTS/GOTS technology into the tactical warfighter arena.

# JW-101 *Defense Messaging System*

**Sponsor:** MAJ Calvin Lawyer, USA DISA DMS PMO, Comm (703) 681-0332, DSN 761-0332, E-mail lawyerc@ncr.disa.mil



## Description

- Provides secure, reliable messaging system capable of interoperating with other legacy messaging systems (e.g., Simple Mail Transfer Protocol {SMTP}.)
- Provides DMS connectivity to all participating DMS sites and gateways into additional sites using SMTP based email on the Secret Coalition Wide Area Network (CWAN).
- Provides message traffic to non-DMS users via the Multifunction Interpreter (MFI.).

## Capability Assessment

- DMS is interoperable with legacy message systems (e.g. SMTP).
- DMS messaging operates on the Coalition WAN.
- DMS demonstrated directory services and secure reliable messaging capability.

## Objectives Supported

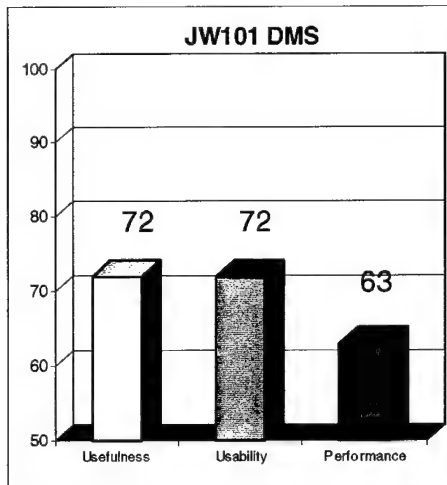
Objective 2 - DMS was able to send common operational pictures (COP) and imagery information as message attachments. Messages were transmitted to and from joint warriors, ashore, afloat, and on the battlefield. Message transfers were accomplished with encryption and authentication of the Multi-Level Information System Security Initiative (MISSI) services.

Objective 5 - DMS provided a messaging communications system with controlled access which allowed the exchange of encrypted and authenticated information via digital signature. Security was provided through the use of Fortezza technology. This technology provided encryption, digital signature, and authentication for message traffic. The DMS infrastructure utilized DMS servers which provided support for JDEF, the Pentagon, and for the coalition forces, NATO, and New Zealand (aboard the USS John C. Stennis). Secure messaging was also provided to the Pentagon.

Objective 6 - DMS is a commercially developed system that integrates military messaging requirements with commercially available products, enabling data exchange in the form of messages and multimedia attachments, as well as directory services among all DMS users.

Objective 7 - DMS is an element of the DII at level 3 compliance.

Objective 9 - DMS co-hosted Microsoft user agent components on the same platform such as the Increased Compression Engine (ICE JW009) application. This allowed the user agent components to be configured for multiple applications on a single platform. DMS also demonstrated its ability to transmit messages to non-DMS users via SMTP.



## Quick Look

- Limited number of nodes operational thus not stressing fully system's capabilities.
- Initially some minor configuration and classification certificate problems.
- Moved message traffic across multiple networks.
- Provided data transfer of binary files.
- Throughout the operation, operators became more familiar and adept with the system.

## Results

**Usefulness – 72%:** DMS was able to provide connectivity with other coalition forces. The operators were able to transmit and receive message traffic from other sites as well as other messaging systems. The system did experience some minor configuration problems with the Multifunction Interpreter (MFI).

**Usability – 72%:** Initially, operators had difficulty understanding the icons, and how to respond to the prompts prior to sending a message. As the operators became more familiar with the system, the easier it became to use and understand.

**Performance – 63%:** DMS was able to demonstrate the movement of message traffic across multiple networks. It utilized the connectivity between the SIPRNET and the CWAN for the data transfer of binary files as message attachments. The data transfer of binary files proved to be a huge success because these files were used by other demonstrations.

## Value Added

The Defense Message System demonstrated it is capable of providing a full email messaging system throughout the wartime scenario with minimum disruption of overall operations. The only disruption would be in the amount of time it would take an operator to learn how to operate his or her DMS user agent.

## Conclusions

The demonstration only supported the National Command Authority (NCA) cell and above, a limited number of nodes. There were some initial setup, configuration and classification certificate problems, but once the corrections were made the system performed flawlessly. The Defense Message System, when fully configured and tested for Warfighter use, has potential to provide the Department of Defense an organizational and interpersonal messaging service, replacing the current AUTODIN system and SMTP based electronic mail.

## Recommendations

- Investigate the Multifunction Interpreter configuration and classification certificate problems.
- Stress the system under realistic operational conditions to fully examine its capabilities prior to replacing current DoD organizational and interpersonal messaging services.
- Develop DMS User Agents for GCCS platforms to allow transfer of messages.

## Warfighter Impressions

- Promising technology.
- Needs to be tested in an operational environment.
- Interoperability with multiple systems' hardware and software will enhance Joint operations.

# JW-106      *Global Combat Support System*

**Sponsor:** LTG John J. Cusick, Director for Logistics, The Joint Staff



## **Description**

- Provides common environment and shared infrastructure required to rapidly deploy integrated combat support capabilities for the warfighter.
- Deliver interoperability "across and between" combat support and C2 functions.
- Expands availability of combat support info to JTF Commander.
- Single workstation access.

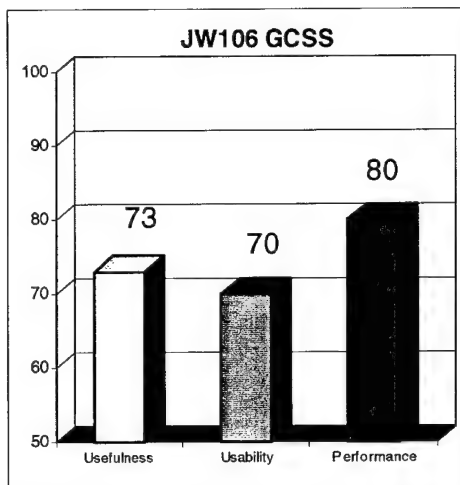
## **Capability Assessment**

- GCSS provided access to multiple applications from a single workstation.
- GCSS provided access to common services via the NIPRNET / SIPRNET networks.
- GCSS enabled functional and cross-functional applications to operate using common services and shared data. Common services include digitized maps, email, collaborative tools access to electronic documents, and drawings, and web services.

## **Objectives Supported**

Objective 8 - Provided an integrated, near-real time logistics focused capability with planning and decision support tools from the Integrated Consumable Item Support (ICIS) model and selected applications from the Logistics Anchor Desk (LAD). GCSS incorporated the ability to track all classes of supply, propositioned war reserves, and personnel to and from the sustaining base and wholesale depots/ home station through incorporation of Joint Total Asset Visibility (JTAV) and Joint Personnel Asset Visibility (JPAV). Additional applications included: Global Transportation Network (GTN), Joint Computer-Aided Acquisition and Logistics Support System (JACLS), Joint Engineering Data Management Information and Control System (JEDMICS), Knowledge-Based Logistics Planning System (KBLPS), and TRANSCOM Regulating and C2 Evacuation System (TRAC2ES).





## Quick Look

- Combines logistics, personnel, maintenance and transportation applications on one workstation.
- Interfaced to GCCS.
- Provides collaborative planning services.
- Operators found system easy to operate.
- Requires knowledge of combat support systems.

## Results

**Usefulness – 73%:** GCSS allowed access to logistics, transportation, and personnel applications from either SPARC or PC based workstations. The Collaborative Virtual Workspace (CVW) supported shared whiteboard, audio video teleconferencing, and email chat rooms. The WEB provided the focal point that allowed the Joint Warfighter to locate, access, and integrate combat support information, applications, and support services. Limited multi-Service logistics data available was in the JWID data base since the demo was on the CWAN.

**Usability – 70%:** Required to enter a password for each application. There are plans to operate GCSS on one network and to automatically enter passwords for each application after the initial one is entered.

**Performance – 80%:** The sites encountered some network problems and some difficulties accessing remote applications. Availability was more consistent with time.

## Value Added

GCSS consolidated multiple existing systems on one workstation with the attendant savings in time, space, and support requirements. GCSS provided for collaborative planning on combat support among sites and facilitated the continuing process of business process reengineering. GCSS has application at the theater (CINC), operational level (CTF commander and Component Commander), and tactical level (NAVFOR-Task Group/ship/unit, ARFOR-division/brigade/battalion, AFFOR-airforce/wing/squadron, MARFOR-expeditionary force/regiment/battalion). Should reduce life cycle costs by facilitating moves from legacy/UNIX based systems to WINDOWS NT based systems.

## Conclusions

The environment and service capabilities of GCSS provided a sound basis for an integrated combat support system. It implemented the focused logistics operational concept of Joint Vision 2010. Problems with the use of legacy applications need to be kept separate from those problems that apply to the environment and services provided by GCSS. Upgrades to applications must resolve human factors issues associated with switching from one application to another and extracting data from one application for use in another. The issues of multiple networks and multiple logins should be resolved before fielding.

## Recommendations

- Expeditiously resolve issues and field.
- Continue improving usability of individual applications and models.

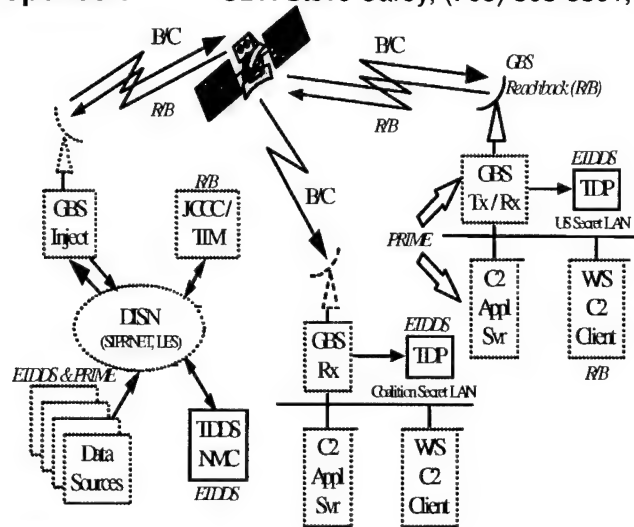
## Warfighter Impressions

- Powerful tool for logisticians.
- A robust, standardized, deployable PC is required for successful use at any echelon.
- Extremely beneficial in the hands of personnel working in a Logistics Readiness Center or an Operations Center environment.
- Valuable system that is needed in the near term.



# JW-112 Enhanced Broadcast Services (EBS) for the Warfighter

**Sponsor:** CDR Steve Carey, (703) 808-6801, careys@oso.nrl.navy.mil



JW112FLPT

## Description

- Provides enhanced services and integration of broadcast services to support tactical forces.
- PRIME provides standard imagery in NITF 2.0 format over open systems architecture.
- IBS-C emulates expanded narrowband capabilities of future IBS.
- GBS Reachback provides highly-asymmetric, two-way comms sharing the GBS broadcast transponder.

## Capability Assessment

- The reachback capability provided a means for requesting retransmission of Global Broadcast Services (GBS) data. This is a new source of bandwidth to the deployed warfighter.
- Primary Imagery Products to Warfare Planners (PRIME) provided the end-user with access control and dissemination (user pull) through use of the reachback capability. PRIME also provided a capability to disseminate primary imagery into an end user's native system, e.g. Precision Target Workstation GCCS.
- Integrated Broadcast Service Concept (IBS-C) provided more tactical data to users, expanding battlespace awareness. Filtering by the end-user allowed the selection of the most relevant mission data..

## Objectives Supported

Objective 2 - Reachback used a single GBS transponder for dual broadcasts to provide a channel for requesting information to be sent over GBS without depending on any other connectivity. PRIME enhanced end user access, control, and dissemination (e.g. "User Pull") of national primary imagery through the use of high bandwidth communications (i.e. GBS, S-ATM).

Objective 3 - GBS Reachback provided a warfighter channel to request information needed for the execution and continuance of the battle. PRIME provided tailored receipt of primary imagery and identified and highlighted specific pre-identified user interest areas and targets.

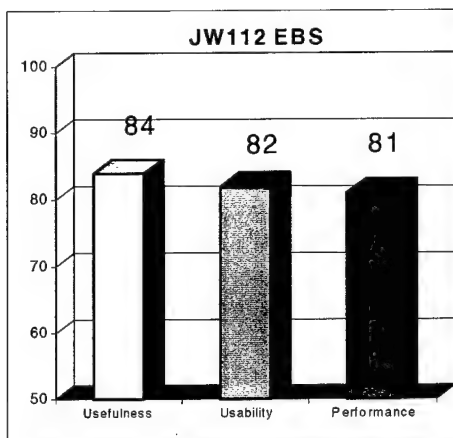
Objective 4 - IBS-C and PRIME provided indications and warning data, cross cueing, and other threat and targeting data. PRIME also provided increased support to the war planner by the use of primary imagery in that operational environment.

Objective 5 - PRIME established first time direct access to primary imagery at the US Secret level to users to allow "disadvantaged" users full use of primary imagery to meet information and battlespace requirements.

Objective 6 - IBS-C and PRIME components were solely COTS/GOTS, GBS Reachback used COTS.

Objective 7 - Demonstrated IBS-C and Reachback functionality extension and utility of the GBS element of the DISN/DII.





## Quick Look

- IBS-C allowed 5-7 times greater data transfer.
- Reachback provided situational awareness with significant increase in data transfer/receipt over one highly asymmetric, two-way satellite dish.
- PRIME provided alternative comm path, selection and end-user access, control and dissemination of primary imagery through use of high-bandwidth data comms.

## Results

**Usefulness – 84%:** IBS-C provided approximately 5-7 times the operational and intelligence information with user filtering. Reachback provided a highly asymmetric, timely and inexpensive 2-way comm path by sharing GBS broadcast transponder.

**Usability – 82%:** Operators were able to effectively use EBS. PRIME software problems mandated both operator and sponsor to interface with UNIX code. The system application or network should be able to notify the operator when new products have arrived and are available in the Image Product Archive (IPA).

**Performance – 81%:** All EBS systems functioned full time to provide the imagery and intel information. Tactical Related Applications (TRAP) Data Dissemination System (TDDS) broadcast, at the GBS injection point, had reset issues causing loss of receive. PRIME's frequency and number of primary imagery products disseminated was limited by the file transfer service throughput of the GBS system. These GBS IP receiver suite limitations were design based on crypto router interface limits.

## Value Added

IBS-C provided user access to larger volumes of files and expanded battlespace awareness for tactical users by near real time display. Reachback provided highly asymmetric, timely two way comm directly through GBS. PRIME enabled cost effective direct ordering and delivery of primary imagery at lower operational levels.

## Conclusions

IBS-C provided additional data that had significant potential operational benefit. The volume of information passed was a great benefit to the warfighter. The ability to filter information at receive terminals precluded overload by individual users while simultaneously ensuring user immediate access to the required data. GBS Reachback could support multiple users with lower bandwidth needs. Use of the PRIME standards-based and open systems architecture for disseminating primary imagery significantly broadened availability of these products to lower echelons where operational strike planning could be conducted.

## Recommendations

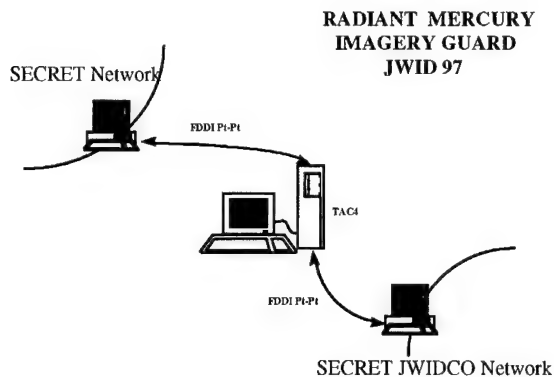
- Continue IBS-C participation in field exercises to refine applications and provide near-term limited operational capability for SIPRNET reachback.
- Integrate reachback in GBS concept of operations. Pursue bandwidth and CDMA technology to allow multiple facilities.
- Initiate a near-term limited PRIME fielding to refine the end-to-end processes and procedures. Accelerate on-line automated US Secret-level interface to the principal imagery source.
- Follow-up PRIME 3-D capability in subsequent assessments; provide results to NIMA as planned evolution towards open systems architecture based on commercial standards.
- Integrate Appliqué, other chat/VTC and MS Office functionality.

## Warfighter Impressions

- IBS-C allows SA and COP data to be provided to small units.
- Ability for GBS "User Pull", without using existing tactical comms, is a great benefit.
- GBS Reachback provided tailored info to a particular user.
- Availability of tailored primary imagery data will provide aircraft and missile strike planning.

# JW-123 *Radiant Mercury Imagery Guard (RMIG)*

**Sponsor:** Judy Bednar, CNO N62, Comm 703.697-6865, E-mail: bednarj@smtp-gw.spawar.navy.mil



## Description

- Multi-level security (MLS) rule-based system that provides automatic security screening and guarding of NITF images.
- Allows imagery to be moved quickly from one security level to a lower or foreign releasable level in less than 30 seconds per image.

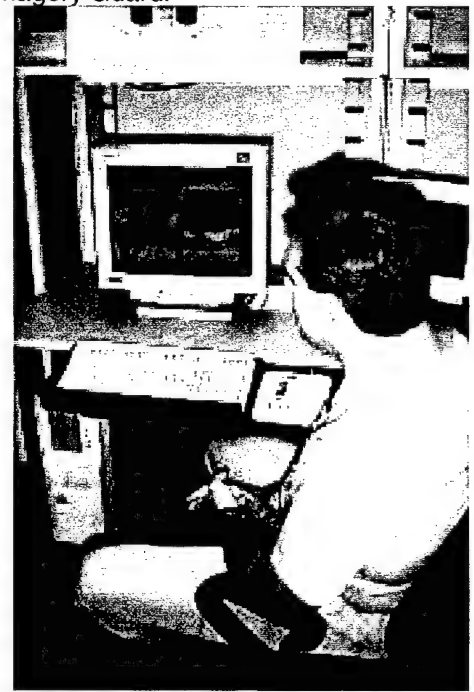
## Capability Assessment

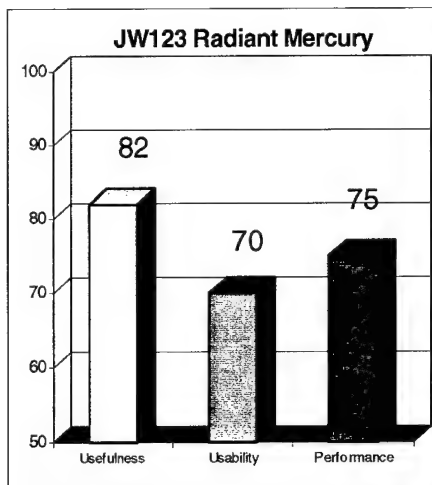
- Radiant Mercury Imagery Guard (RMIG) allowed ISR images with National Imagery Transmission Format Standard (NITFS) headers to be automatically transferred across security levels within a command and between coalition partners.
- RMIG prevented images, which did not meet its trusted and accredited rule set, from being moved from one security level to another.
- The exchange of imagery between multiple levels of security was near real time and seamless for US and coalition forces and supported collaborative planning.
- RMIG was complete and simple in its implementation as an automatic Imagery Guard.
- RMIG was 100% accurate in its passing and rejection of imagery selected to be passed from one security level to another.
- RMIG was straight forward to operate and easy to learn.

## Objectives Supported

Objective 1 - Enabled the real-time dissemination of downgraded imagery across security levels from the SIPRNET to the Coalition Network. This was done on demand as individual operators on the SIPRNET were able to identify specific images that were to be released to the Coalition. The images were automatically screened for the proper NITFS header and automatically transferred across the boundary from one network to the lower classification network.

Objective 2 - Successfully demonstrated the ability to manage imagery that enhanced data delivery to and from Joint Warriors and coalition partners.





## Quick Look

- Proved capability to pass US imagery residing on US only system to Coalition forces automatically.
- Performed all stated functional capabilities.
- Allowed all releasable images to be passed across security levels and between the coalition.
- Prevented all images which did not meet the trusted and accredited rule set from being transferred from one security level to another.
- Rapidly transferred images (15 to 20 seconds) from SIPRNET to GWAN for all US command levels and coalition forces.

## Results

**Usefulness – 82%:** The RM system is complete and simple in its implementation. Operators and Staff were able to quickly implement the full capability of the demonstration. RM-passed images were available to all other systems on the Coalition Network for their use in collaborative planning.

**Usability – 70%:** Operators and assessors were comfortable in operating the RM Imagery capabilities once the configuration was established. Operation was straight forward and easy to learn. RM Imagery Guard provided information consistent with other systems. The RM functional capabilities were provided through JDISS terminals and while, the RM system and functionality were always available, the JDISS terminal usage was so high that RM Operators had a hard time gaining terminal time to operate the RM Imagery Guard.

**Performance – 75%:** The system was able to pass images throughout the demonstration period.

## Value Added

The value added functionality of RM Imagery Guard is the ability to pass US imagery residing on US only systems to Coalition forces automatically. This capability currently does not exist and while other systems are in development, such as C2 Guard, RM has the ability to provide this much needed capability.

## Conclusions

RMIG was well accepted by the Operators and Staff with a simple and easy to use file-transfer-protocol to move images from the image server on the SIPRNET to the RM Imagery Guard Server. Automatic screening of NITF header information made the system easy for the Coalition Warrior to accomplish his/her mission with little training. Concerns may be in the initial setup and configuration of the RM Guard Server itself and the updating of the screening Rule Set. These issues were not addressed in the operational demonstration of the RM Guard Server. The ability of an operator to modify the NITF header information was another issue. In trying to test the RM Imagery Guard capabilities with non-canned (pre-prepared) imagery, it appeared that NITF headers could be manipulated by an operator in order to comply with the RM Rule Set which may not be a fallacy of RM, but may point out a fallacy and vulnerability of NITF.

## Recommendations

- Field system now as a capability for passing imagery between multiple security levels.
- Field as a central server/site for multiple users to pass imagery to reduce individual RM system requirements.

## Warfighter Impressions

- Very effective tool.
- Would take this system to the field now.
- To effectively work in a NATO environment, this capability is a must.
- It provides a capability that currently does not exist and the automation ensures timely delivery.

(This page is intentionally left blank.)

## SECTION 3 - CONCLUSIONS AND RECOMMENDATIONS

This section of the report contains the high level conclusions and recommendation for all demonstrations and identifies which of these demonstrations shows potential in providing value added to the warfighter. Each of these demonstrations has been rated on its usefulness, its usability, and its performance as defined in the assessment methodology section contained in section 1.5. Each of these criteria were measured separately. Results of this assessment are presented in figure 3-1.

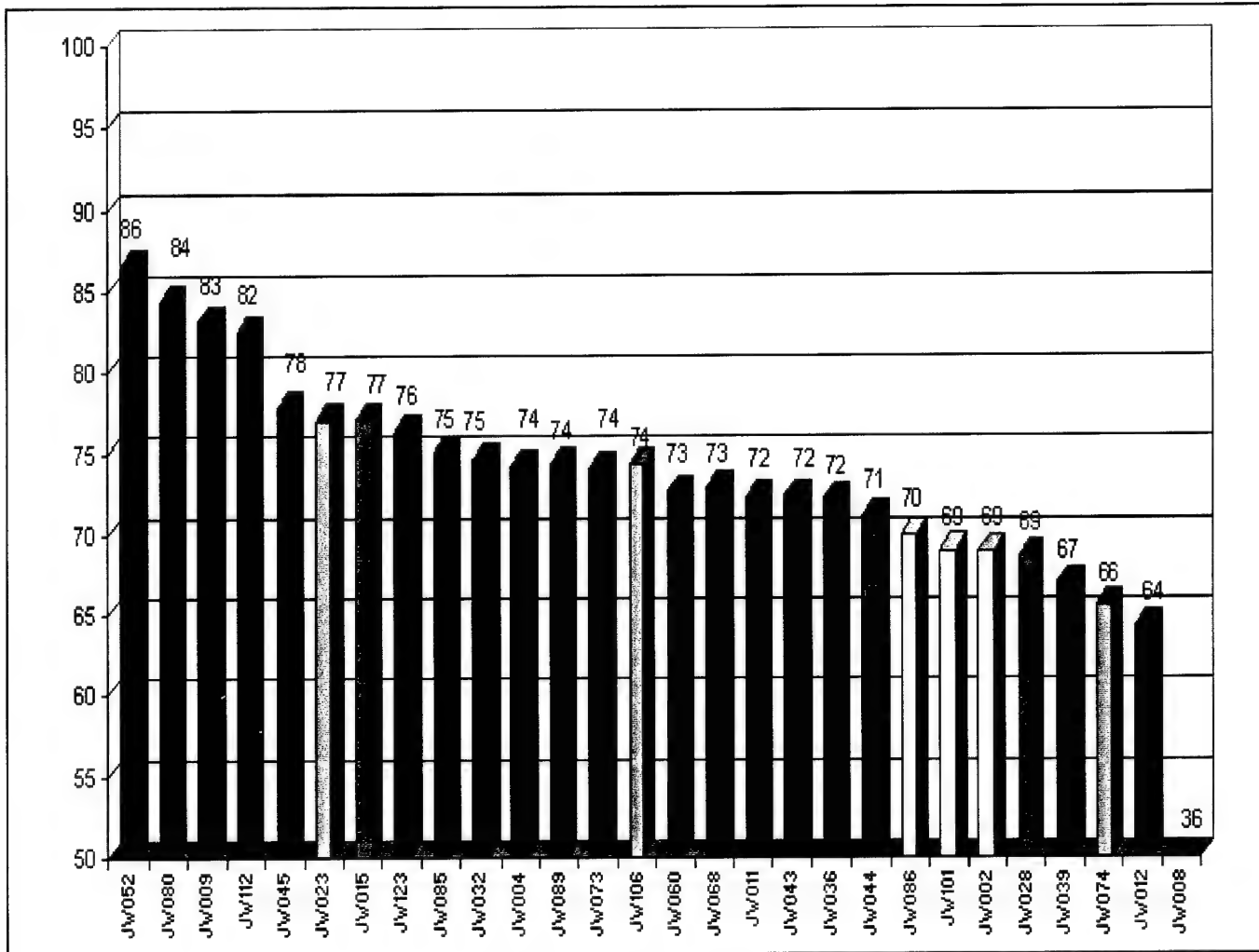


Figure 3-1. Overall Ratings

### 3.1 Candidates for Implementation

The top ten rated demonstrations are recommended as candidates for accelerated development and procurement as a result of the warfighter assessment. They are grouped into three categories: a) Gold Nuggets, b) enhancements to existing systems, and c) new technologies. A brief description of each category and the value added by the demonstrations from the warfighter's perspective is addressed below.

#### 3.1.1 Gold Nuggets

Four demonstrations were identified as Gold Nuggets. Gold Nuggets are demonstrations that were rated by the warfighter to have value added and will be ready to be fielded within six months. These demonstrations are discussed below.

Increased Compression Engine (ICE) (JW009) - ICE provided an imagery compression, transfer, and analysis tool to increase quality and compression performance. Images were compressed by a factor of up to 150:1 for color; up to 100:1 for grayscale. This was accomplished over low bandwidth communication links while retaining critical image details for analysis and intelligent decision making. ICE provided value added to the warfighter by allowing transfer of large imagery data files which were compressed using less bandwidth for transmission. Imagery specialists used the Visual National Imagery Interpretability Rating Scale (NIIRS) to judge the clarity of the images. ICE compressed images normally only lost one NIIRS level of clarity as a result of the compression technique. Normally an image in its original state would take twenty to thirty minutes to push through or pull through a 9.6 modem line. The same compressed image could be pushed or pulled through the same 9.6 modem in 1-2 minutes.

Modeling and Simulation Support to C4I in the DII COE Warfighting Environment (COMPASS PHASE II) (JW023) - JW023 provided a package of software programs that brought Modeling and Simulation (M&S) services supported by Distributed Collaborative Planning (DCP) tools to the task of writing plans for the CTF. COMPASS PHASE II provided for a wide range of DII COE compliant C4I systems to interface with legacy M&S services which are non-DII COE compliant. The demonstration provided analysis, preview, and rehearsal capabilities of M&S system results that could transform C4I systems into collaborative planning, rehearsal, and training systems. COMPASS PHASE II provided value added to the warfighter by accessing legacy modeling and simulation systems and providing Distributed Collaborative Planning (DCP) tools to support planning assessment, review, revision, rehearsal, and post action analysis of plans. and modeling of missions.

Submarine Joint Coalition Combat Operations (JW080) - JW080 provided the capability for a submarine to pass real-time imagery, enhance data delivery, and integrate sensor-to-sensor and sensor-to-shooter technologies. It combined the submarine's inherent stealth, mobility, and firepower with an Advanced Common Operating Picture (ACOP). Both Telemedicine and SWAMPS provided value added capabilities that were never demonstrated before. The Telemedicine system provided the submarine Independent Duty Corpsman (IDC) access to medical expertise not previously available to a deployed underway submarine. This was both a time saver and a potential life saver. SWAMPS was used to conduct post mission intelligence briefings to the CCTF on USS John C Stennis from Seals on the USS Atlanta using line of sight antennas while in transit.



Whiteboard, Chat Box, maps, imagery, and charts were used to show the specific locations of mines and water obstacles in real-time. JW080 provided enhanced data delivery to and from Joint Warriors at the unit level, particularly medical information and common operational picture and imagery, between ships and submarines at sea.

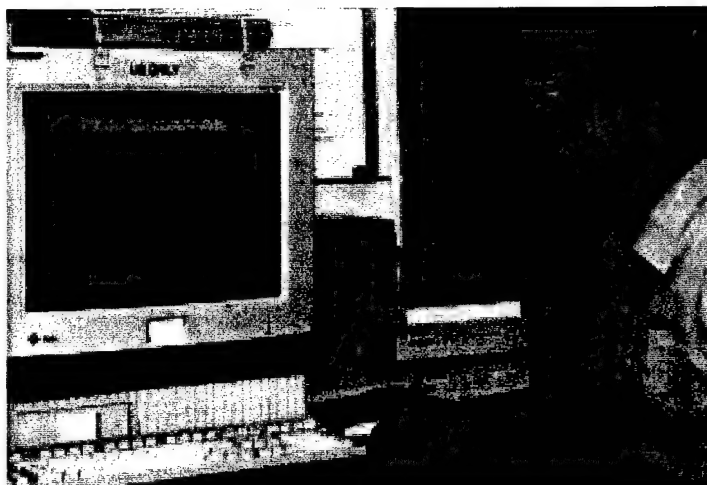
Radiant Mercury Imagery Guard (RMIG) (JW123) - RM is a multilevel security system which enables Intelligence, Surveillance and Reconnaissance (ISR) images with NITF-S headers to be automatically transferred across security levels within a theater of operations and to coalition partners. The value added functionality enabled by RMIG Imagery Guard was the ability to automatically pass US imagery residing on US only systems to Coalition forces. This capability currently does not exist and, while other systems are in development, such as C2guard, RM provides an interim solution.

### **3.1.2 Enhancements to Existing Systems**

Three of the top ten demonstrations are enhancements to existing systems. These demonstrations were judged by the warfighter to have value added and are part of the a continuing funded program. These demonstrations are discussed below.



DII-Based Joint Deployable Intelligence Support System (JDISS) (JW015) - JDISS is an integrated family of plug-in intelligence support and multimedia collaborative software segments based on DII COE, and COTS Multi Level Security (MLS) and Trusted Web technology that allow the secure exchange of intelligence data and multi-security level access to web-based products and data. The primary value-added was the ability to pass information from one security level network to another through a man-in-the-loop control point to oversee the movement of the information between the SIPRNET, LOCE and CWAN networks.



It allowed the operator to quickly and efficiently move intelligence products which automatically ties capabilities and performance between these networks. It is an improvement over the current Operations-Intelligence Workstation (OIW), because it can handle up to 13 networks while OIW can only handle 2. JDISS provided a critical MLS capability for coalition operations by preventing low side users from accessing any high side data. MLS proved to be a time-efficient, yet secure method for dissemination of large or continuous amounts of information to a coalition that operates at different security levels.

Integrated Situation Awareness (ISA) (JW085) - ISA provided the warfighter the Common Operational Picture (COP), integrated Intelligence, Surveillance and Reconnaissance (ISR) and Meteorological and Oceanographic (METOC) data into the COP, and provided ISR sensor management and sensor performance assessment tools to support improved situational awareness, mission planning and sensor tasking. ISA provided added value with new retrieval, display, and distribution capabilities, which included: a) Tailorable COP with filtering and compression to submarines and other low-bandwidth units; b) Introduction of enhanced display of the Ground Order of Battle highlighting the new PLI Server called EPLIS; c) Battlefield roll-up and spread display option to view multiple small land units, a C2PC to distribute the COP to PC users at both LAN and WAN sites using the C2PC gateway; and d) ELVIS II COP browser enhanced with a JAVA display and collaborative training capability. The ISA provided improved Intelligence, Surveillance, and Reconnaissance (ISR) sensor management and performance assessment tools, which included: access to JSTARS and Predator Video; the ability to link ISR assets/functionality together into a system; the ability to display sensor coverage maps and performance assessment for blue force and national sensors; an enhanced air picture data to current air tracks; Sensor Status Reporting System providing increased functionality and implementation; and a dedicated TMD warning capability from Air Force Space Warfare Center to the Task Force. Upgrades to the Joint METOC Segment (JMS) of the GCCS included a user selectable information display on the COP terminal (CWAN only) showing the METOC impact to operations.

Enhanced Broadcast Services (EBS) for the Warfighter (JW112) - EBS demonstrated enhanced services, technology, and integration of broadcast services in support of tactical forces. This demonstration consisted of three distinct segments: a) Integrated Broadcast Service Concept (IBS-C) (formerly Extended TRAP Data Dissemination System (ETDDS)), b) Global Broadcast Service (GBS) Reachback, and c) Primary Imagery Products to Warfare Planners (PRIME). The IBS-C broadcast enabled additional categories of data to be broadcast, providing more information to the users and ensuring that a wider range of users received their highest priority data. GBS Reachback was a technology prototype to provide highly-asymmetric bi-directional simplex mode (two separate and independent channels - one each way) communications directly through the GBS. PRIME demonstrated an infrastructure for the delivery of primary imagery in a standards-compliant format (National Imagery Transmission Format Standard (NITFS) 2.0) over an open-systems architecture. IBS-C provided value added by allowing a wider range of user access to larger volumes of files and provided expanded battlespace awareness for disadvantaged tactical users by producing principally NRT display on users' enhanced tactical data processors (ETDPs). Reachback made available a timely two-way communications path directly through GBS which provided essential user-pull of information with less equipment and less infrastructure connectivity. PRIME enabled direct ordering and delivery of primary imagery to JWID components at lower operational levels which provided better support strike missions.

### 3.1.3 New Technologies

Three of the top ten demonstrations used new technologies to meet warfighter requirements. These demonstrations were judged by the warfighter to have value added and but require more that six months of continued development . These demonstrations are discussed below.

Situational Awareness Beacon with Reply (SABER) (JW032) - SABER supported the Joint Warfighter by providing real-time Position Location Information (PLI) derived from the Global Positioning System (GPS) and platform data. SABER supported Combat Identification (CID) by combining friendly force Situational Awareness (SA) information reported by the beacon with direct network query of real-time friendly combat unit GPS positions. SABER supported the Enhanced PLI segment (EPLIS) and the Joint Maritime Communications Information System (JMCIS) in the JW085 Common Operational Picture (COP) demonstration. SABER provided added value by enhancing the Tactical Commander's ability to accomplish his mission by providing two critical elements for maneuvering combat units: a) Friendly identification from a direct query of the SABER network before firing into an area and b) Real-time automatic updated blue force SA. As a safety device to help prevent fratricide, SABER provided enhanced CID information to the warfighter. SABER is an added value tool for C2 because it eliminated the requirement for manual plotting of old unit information. At the tactical level, SABER enhanced the ability to navigate and rendezvous with other tactical units. SABER assisted the Commander with key decisions that involved maneuver, commitment of forces/reserves and the potential loss for life from a possible fratricide situation when engaging enemy forces close to friendly units.

Imagery and Geospatial Support (JW045) - The Imagery and Geospatial Support (IG&S) demonstration was a proof-of-concept for a US Imagery and Geospatial System (USIGS) functionality, and Warfighter interface into a common, imagery, imagery intelligence, and geospatial environment (database). The IDM and C2 Guard provided added value by allowing the user the ability to pull



imagery and geospatial information from a US-only network to an allied or coalition environment. Previously, the only way to gain imagery and geospatial data was via hard copy, which takes on the order of weeks to be authorized. Imagery analysts do not currently have the ability to incorporate their products with common operating picture systems without having to manually input corner points and manually manipulate the data which introduces operator error and precious time. Planners and decision-makers have the capability to view the targets or current capabilities of the opposing forces in a timely fashion and observe any new routes or changes in a moments notice. The different CIB images, NITF images, vector data, and other geospatial products (and the ability to view predator UAV feeds) enabled the Warfighter to view the scene minutes prior to the mission for the most up to the minute information.

Information Operations (IO) Defense and Information Battle Damage Assessment (I-BDA) (JW052) - Information Operations (IO) Defense and Battle Damage Assessment (BDA) demonstrated the ability to detect, analyze, and defend against offensive IO. It used the Automated Security Incident Measurement (ASIM) device to detect unauthorized intrusions, the Automated Computer Examination System (ACES) to track, analyze, and determine the nature and extent of the intrusion, and the ENVOY visualization tool to integrate ASIM and ACES data. JW052 provided defense information systems the ability to lock out subsequent intruder attempts through early detection, damage assessment, and notification. The primary value-added was the integration of ASIM and ACES through ENVOY. ASIM is currently in use by all three Information Warfare Centers and ACES, is a proven system and is used by the FBI. ENVOY provided a new capability and allowed the integration and visualization of data from two proven intrusion detection tools (ASIM and ACES). This simplified the analysis process and allowed operators with little or no intrusion detection experience to quickly and efficiently determine the nature and extent of the intrusion.

## 3.2 Issues

---

Several issues were identified which should be addressed. The highlights from the issue area are discussed below.

CWAN provided necessary infrastructure to support Coalition operations, but there remain some unresolved MLS issues - The JWID 97 implementation of the CWAN proved the concept of an operational multinational network that supported network centric coalition operations. It demonstrated the feasibility of providing an infrastructure that supported multiple communities of interest on a single network and facilitated the timely exchange of data and access to database information. Some issues were identified. First, the MLS systems were not available for all information transfer. To work around this, many participants established partial databases on the CWAN. These databases were not always complete. As a result demonstrations could not show all capabilities. Second, data element labeling was not standardized. As a result MLS algorithms could not determine releasability of information, Standard data element labeling conventions are required for the efficient utilization of MLS techniques.

Email concept proved valuable, but requires procedures, policy and discipline - Email provided a viable means to pass messages and information between the CCTF and the components. This shift away from the traditional message processes like AUTODIN is occurring without the procedures, policy and discipline associated with the old system. Email provided a familiar environment for most warfighters to work in, but in a tactical situation, some of the traditionally procedures did not work. Addressing by function and organization was not accomplished and personal email accounts names were used in a broadcast mode which resulted in large volumes of traffic. New policy, procedures, and discipline need to be developed to support this environment.

Collaborative tools still not standardized - The collaborative tools used in JWID 97 demonstrations were, for the most part, not compatible with each other. This meant that while demonstrations could collaborate within themselves at various sites, they did not collaborate between systems. There has been a recommendation to standardize collaborative tools in the last two JWIDs.

## 3.3 Recommendations

---

- Field the "Golden Nuggets" and exploit identified technologies that provide value added.
- Make interoperability in Coalition Operations a reality by resolving MLS issues and obtaining NSA accreditation.
- Standardize data element labeling to enhance use of databases in operational environments.
- Standardize distributed collaborative planning tool and use those that will interact between systems as well as within systems.



(This page intentionally left blank)

## *APPENDIX A - ACRONYM LIST*

---

ACES	Automated Computer Examination System
ACOM	Atlantic Command
ACOP	Advanced Common Operating Picture
ADNS	Automated Digital Network System
ADS	Advanced Distribution Simulation
ADS	Airspace Deconfliction System
AF	Air Force
AFATDS	Advanced Field Artillery Tactical Data System
AFFOR	Air Force Forces
AGCCS	Army GCCS
AIC	Atlantic Intelligence Command
AOC	Air Operations Center
AOR	Area of Responsibility
APS	Advanced Planning System
ARFOR	Army Forces
ASIM	Automated Security Incident Measurement
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
AUTODIN	Automatic Digital Information Network
BADD	Battlefield Awareness and Data Dissemination
BATES	Battlefield Artillery Target Engagement System (UK)
BSC	Base Station Controller
BVTC	Battlefield VTC
C2	Command and Control
C2G	Command and Control Guard
C2I	Control and Intelligence
C2PC	Command and Control Personal Computer
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAOC	Coalition Air Operations Center
CAP	Collaborative Action Planning
CCCC	Coalition Communications Control Center
CCITT	Consultative Committee for International Telegraph & Telephone
CCTF	Commander Coalition Task Force
CDMA	Code Division Multiple Access
CDT	Computer Display Terminal
CIB	Controlled Image Base
CID	Combat Identification
CINC	Commander in Chief
CINCUSACOM	Commander In Chief United States Atlantic Command
CIS	Combat Intelligence System
CJCSI	Commander Joint Chiefs of Staff Instruction
CJTF	Coalition Joint Task Force
COE	Common Operating Environment
COMPASS	Common Operational Modeling Planning and Simulation Strategy
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial off-the-shelf
CSNI	Communications System Network Infrastructure
CTAPS	Contingency Theater Automated Planning System

CTF	Coalition Task Force
CVW	Collaborative Virtual Workspace
CWAN	Coalition Wide Area Network - Secret
D/D	Deployable Distributed
DAMA	Demand Assigned Multiple Access
DARPA	Defense Advanced Research Projects Agency
DCP	Distributed Collaborative Planning
DEMUX	Demultiplexer
DII	Defense Information Infrastructure
DII COE	Defense Information Infrastructure Common Operating Environment
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN/DII	Defense Information Systems Network/Defense Information Infrastructure
DMS	Defense Message System for the Warfighter
DNVT	Digital Nonsecure Vehicular Telephone
DoD	Department of Defense
DSN	Defense Switch Network
DSS	Depot Standard System
DTG	Digital Trunk Group
EAFTDS	Enhanced AFATDS
EBS	Enhanced Broadcast Services
ECOP	Enhanced Common Operational Picture
EHF	Extremely High Frequency
ELINT	Electronic Intelligence
EMCON	Emission Control
ENVOY	Visualization tool
EPLIS	Enhanced Position Locator Information System
EPS	Equipment Planning System
ERGM	Extended Range Guided Munitions
ETDP	Enhanced Tactical Data Processing
FATDS	Field Artillery Tactical Data Systems
FE	Forward Eagle
FID	Friendly Identification
FLEX	Force Level Execution
FTP	File Transfer Protocol
GBS	Global Broadcast System
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GOTS	Government off-the-shelf
GPS	Geographical Positioning System
GTN	Global Transportation Network
HMMWV	High Mobility Multipurpose Wheeled Vehicle
HSMUX	High Speed Multiplexer
IG&S	Imagery and Geospatial Support
IBDA	Information Battle Damage Assessment
IBS-C	Integrated Broadcast Service Concept
ICE	Increased Compression Engine
ICIS	Integrated Consumable Item Support
ID	Identify
IDC	Independent Duty Corpsman
IDM	Information Dissemination Management server
IO	Information Operation
IOT&E	Initial Operational Test and Evaluation
IP	Internet Protocol
IPA	Image Product Archive
IR	Infrared



ISA	Integrated Situational Awareness
ISDN	Integrated Services Digital Network
ISR	Intelligence, Surveillance and Reconnaissance
ISRD	ISR Sensor Management (Integrated Situation Awareness)
IW	Information Warfare
JACCS	Joint Attack Command and Control System
JBC	Joint Battle Center
JCA	Joint Countermine Applications
JCM	Joint Counter Mine
JCALs	Joint Computer-Aided Acquisition & Logistics Support System
JCSE	Joint Continuous Strike Environment
JDEF	Joint Demonstration and Evaluation Facility
JDISS	Joint Deployable Intelligence Support System
JEDMICS	Joint Engineering Data Management Information & Control System
JFACC	Joint Forces Air Component Commander
JIC	Joint Intelligence Center
JIGI	JSTARS Imagery Geolocational Improvement
JINC	Joint Internet Controller
JITC	Joint Interoperability Test Command
JMCIS	Joint Maritime Command Information System
JMCOMS	Joint Maritime Communications Systems
JMS	Joint METOC Segment
JOPEs	Joint Operation Planning and Execution System
JPAV	Joint Personnel Asset Visibility Management Information System
JPEG	Joint Photographic Experts Group
JPO	Joint Program Office
JPT	Joint Planning Tool
JROC	Joint Requirements Oversight Council
JSOTF	Joint Special Operations Task Force
JSTARS	Joint Surveillance Target Attack Radar System
JTASC	Joint Training Analysis and Simulation Center
JTAV	Joint Total Asset Visibility Management Information System
JTF	Joint Task Force
JWID	Joint Warrior Interoperability Demonstration
KBLPS	Knowledge-based Logistics Planning System
LAD	Logistics Anchor Desk
LAN	Local Area Network
LCAC	Landing Craft Air Cushion
LES	Leading Edge Services
LMST	Lightweight Multi-band Satellite Terminal
LOCE	Operations-Intel Center Europe
LOS	Line of Sight
M&S	Modeling and Simulation
MARFOR	Marine Corps Forces
MCM	Multimedia Collaborative Manager
MCTC	Mine Countermeasures Technical Center
MDX	Message Data Exchange
MECCS	Mobile Expeditionary Cellular Communications Site
MEDEVAC	Medical Evacuation
MET	Multi-image Exploitation Tool
METOC	Meteorological and Oceanographic
MFI	Multifunction Interpreter
MILSTAR	Military Satellite Network
MISSI	Multi-level Information System Security Initiative
MLS	Multi-Level Security
MNTG	Multi-National Task Group
MNW	Multi Network Workstation
MSE	Mobile Subscriber Equipment

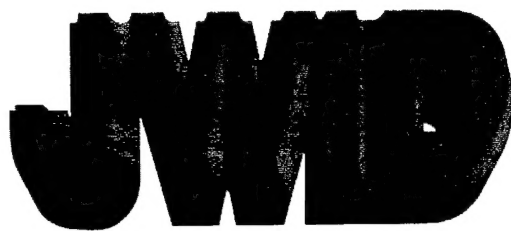
MSEL	Master Scenario Events List
MSLS	Multi Security Level Server
MSRT	Mobile Subscriber Radio Telephone Terminal
MTI	Moving Target Indicator
NATO	North Atlantic Treaty Organization
NAVFOR	Navy Forces
NCA	National Command Authority
NCS	National Command System
NES	Network Encryption Systems
NIIRS	National Imagery Interpretability Rating Scale
NIMA	National Imaging and Mapping Agency
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NITF	National Imagery Transmission Format
NITF-S	National Imagery Transmission Format Standard (NITFS 2.0)
NRaD	Naval Research and Development Laboratory
NRT	near-real-time
NSA	National Security Agency
NSFS	Naval Surface Fire Support
NWCS	Naval Weapon Control System
OIW	Operational Intelligence Workstation
OPFAC	Operational Facility
OPNOTES	Operational Notes
OPORD	Operations Order
ORSMC	Off Route Smart Mine Clearance breaching system
OS	Operating System
PAD	Patient Administration
PLI	Position Location Information
PPK	Paralon PathKey
PRIME	Primary Imagery Products to Warfare Planners
RAAP	Rapid Application of Air Power
RAP	Recognized Air Platforms
RAU	Radio Access Unit
RM	Radiant Mercury
RMIG	Radiant Mercury Imagery Guard
RTCPs	Real-time Collaborative Pre-Strike
SA	Situation Awareness
SABER	Situational Awareness Beacon with Reply
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SBO	Split-Base Operations
SEN	Small Extension Node
SGI	Silicon Graphics Inc.
SHF	Super High Frequency
SIGINT	Signal Intelligence
SIPRNET	Secret Internet Protocol Router Network
SJCCO	Submarine Joint Coalition Combat Operations
SMTP	Simple Mail Transfer Protocol
SMU	Switch Multiplexer Units
SNMP	Simple Network Management Protocol
SOF	Special Operations Forces
SWAMPS	Special Warfare Automated Mission Planning System
TACFILE	Tactical File
TacPCS	Tactical Personal Communications Systems
TADIL-J	Tactical Digital Information Link - J
TAMPS	Tactical Air Mission Planning System
TBM	Theater Ballistic Missile

TBMCS	Theater Ballistic Missile Control System
TBMD	Theater Ballistic Missile Defense
TCO	Tactical Combat Operations
TCP/IP	Transmission Control Protocol/Internet Protocol
TCS	Tactical Control System
TCSdb	Trusted Coalition Scenario Database
TCTA	Time Critical Targeting Aid
TDC	Theater Deployable Communications
TDDS	Tactical Data Dissemination System
TED	Trunk Encryption Device
TEL	Transporter Erector Launcher
TGAN	Task Group Area Network
TIDAS	Trusted Intelink Dissemination Access Servers
TMD	Theater Missile Defense
TMSC	TBMD Multi-Source Correlation
TNL	Target Nomination Lists
TOC	Tactical Operations Center
TRANSEC	Transmission Security
TRAP	Tactical Related Applications
TRE	Tactical Receive Equipment
TRI-TAC	Tri-Service Tactical Communications Program
TS/SI	Top Secret/Sensitive Information
UAV	Unmanned Aerial Vehicle
UHF	Ultrahigh Frequency
UHF LOS	Ultrahigh Frequency, Line of Sight
USACOM	United States Atlantic Command
USIGS	United States Imagery and Geospatial System
USMC	United States Marine Corps
USMTF	United States Message Text Format
UUV	Unmanned Under-water Vehicle
VIP	Very Important Person
VMF	Variable Message Format
VSAT	Very Small Aperture Terminal
VTC	Video Teleconferencing
WAN	Wide Area Network
WFA	Warfighter's Associate workstation
Y2K	Year 2000

(This page left intentionally blank.)



*JWID enhances the Warfighter's ability to plan, coordinate, and execute the mission by demonstrating relevant evolving technology to decision makers; solutions that are specific and focused; and interoperability in a Joint and Coalition environment*



*which results in the integration of appropriate technologies into the Joint Warfighter Capabilities Assessment (JWCA) and the Joint Requirements Oversight Council (JROC) processes*

